

# DataSMART<sup>®</sup> MAX<sup>™</sup> T1/FT1 Multimedia Access User's Guide

---

72761 DataSMART MAX T1  
Dual-Port, Add/drop  
AC power  
72765 DataSMART MAX T1  
Dual-Port, Add/drop  
DC power  
72771 DataSMART MAX T1  
Quad-Port, Add/drop  
AC power  
72775 DataSMART MAX T1  
Quad-Port, Add/drop  
DC power

Document #5000201



**Copyright**

© 1995, 1996, 2001 by Kentrox, LLC. All Rights Reserved.  
Printed in the U.S.A.

Specifications published here are current or planned as of the date of publication of this document. Because we are continuously improving and adding features to our products, Kentrox reserves the right to change specifications without prior notice. You may verify product specifications by contacting our office.

In no event shall Kentrox be liable for any damages resulting from loss of data, loss of use, or loss of profits. Kentrox further disclaims any and all liability for indirect, incidental, special, consequential or other similar damages. This disclaimer of liability applies to all products, publications and services during and after the warranty period.

**Trademark information**

Kentrox and DataSMART are registered trademarks of Kentrox, LLC.  
DataSMART MAX and DataSMART SPort are trademarks of Kentrox, LLC.

All other product names are trademarks or registered trademarks of their respective owners.

**Revision history**

Part #	Date	Description
65-72561101	March, 1995	Issue 1
65-72561102	March, 1995	Issue 2
65-72561103	February, 1996	Issue 3
5000201	December, 2001	Issue 4

# Contents

---

	<b>Preface</b> .....	9
<b>Chapter 1</b>	<b>Introduction</b>	
	Some examples of applications .....	14
	Fractional T1 and Frame Relay .....	14
	DSU .....	14
	DSU with add/drop .....	15
	Features of the DataSMART MAX Multimedia Access Multiplexer.....	16
	A front-panel interface for easy installation.....	16
	All models support all standard data interfaces.....	16
	SNMP-based network management .....	17
	Facility data link .....	18
	T1 performance monitoring .....	18
	T1 diagnostics .....	19
	Nonvolatile memory .....	19
	Using the DataSMART MAX .....	20
	Using the command-line interface.....	20
	Using the front-panel interface .....	21
	Logging in.....	26
	Through the control port: stand-alone.....	26
	Through the control port: daisy-chained.....	26
	Through the FDL.....	26
	Telnet access.....	26
	Front panel .....	26
	Logging out.....	27
<b>Chapter 2</b>	<b>Establishing system security</b>	
	Securing the command-line interface .....	30
	Adding a password .....	31
	Deleting a password .....	31
	Entering a password .....	32
	Viewing a user's access level.....	32
	Viewing the current passwords .....	32
	Securing the front panel .....	33
	Setting the front-panel password.....	34
	Enabling/disabling the front panel.....	35
	Setting auto-logout for the front panel .....	36

## Chapter 3    **Configuring the system**

Specifying system parameters .....	38
Command-line access .....	38
Front-panel access .....	38
Viewing the current settings .....	39
Setting date and time .....	40
Naming the device .....	42
Specifying an address .....	43
Enabling/disabling the front panel .....	44
Specifying DataSMART compatibility .....	44
Specifying the system clock .....	44
Setting auto-logout for the control port .....	48
Setting auto-logout for the front panel .....	49
Zeroing all counters .....	50
Obtaining product version information .....	51
Resetting to default values .....	51
Configuring the control port .....	53
Command-line access .....	53
Front-panel access .....	54
Viewing the current configuration .....	54
Configuring the physical connection .....	56
Enabling/disabling character echo .....	57
Specifying the control port .....	57
Configuring alarms .....	59
Command-line access .....	59
Front-panel access .....	60
Viewing the current configuration .....	60
Enabling/disabling alarm messages .....	61
Formatting the alarm messages (ASCII or SNMP) .....	62
Enabling/disabling alarms on incoming yellow .....	63
Setting the threshold for errored seconds (ES) .....	64
Setting the threshold for unavailable seconds (UAS) .....	65
Specifying the threshold evaluation window .....	66
Setting the alarm deactivation time .....	67

## Chapter 4    **Configuring interfaces**

Configuring the network interface .....	70
Command-line access .....	70
Front-panel access .....	70
Viewing the current NI configuration .....	71
Specifying NI framing format .....	71
Specifying NI line coding .....	73
Enabling/disabling T1.403 loopback and PRM generation .....	74

Enabling/disabling yellow alarm output .....	75
Selecting the 54016 address .....	76
Enabling/disabling 54016 mode .....	77
Specifying transmit line build out attenuation .....	78
Configuring the terminal interface .....	79
Command-line access .....	79
Front-panel access .....	79
Viewing the current TI configuration .....	80
Specifying TI framing format .....	80
Specifying TI line coding .....	81
Specifying TI idle code .....	82
Specifying TI signal equalization .....	83
Configuring data ports .....	85
Command-line access .....	85
Front-panel access .....	85
Viewing the current data port configuration .....	86
Enabling/disabling data inversion .....	87
Specifying the electrical interface of each data port .....	88
Specifying data port clocking .....	89
Enabling/disabling transmit clock inversion .....	91
Enabling/disabling receive clock inversion .....	92
Specifying the data port idle character .....	93
Setting up LOS (loss of signal) processing .....	94
Assigning channels .....	96
Rules for assigning channels .....	96
Assigning channels from the command line .....	98
Assigning channels from the front panel .....	102

## **Chapter 5      Performance monitoring**

Accessing the reports from the command-line .....	106
Interpreting the User NI and the User TI reports .....	108
Time intervals in the reports .....	108
Interpreting the Far-end report .....	112
Interpreting the Statistical reports .....	114
Interpreting the Alarm History report .....	118
Interpreting the Carrier NI report .....	119
Accessing reports from the front panel .....	120

## **Chapter 6      Troubleshooting**

Interpreting the front-panel LEDs .....	124
Selecting the data port to monitor .....	124
Monitoring alarm messages .....	128
Examining system status .....	129

Status codes .....	130
Troubleshooting tree .....	134
Troubleshooting alarms .....	134
NI LOS—critical .....	134
TI LOS—critical .....	134
ECF—critical .....	135
NI OOF—critical .....	135
NI AIS—critical .....	135
TI OOF—major .....	136
DP LOS—major .....	136
NI EER—major .....	136
TI YEL—major .....	137
NI YEL—major .....	137
TI EER—minor .....	137
TI AIS—minor .....	138
BPV—minor .....	138
CRC—minor .....	138
Running the self-test diagnostics .....	139
Self-test error messages .....	140
Using the network signal jacks .....	141
Using loopbacks .....	142
Line loopback .....	142
Payload loopback .....	142
Data port loopback .....	143
Local loopback .....	144
Data terminal loopback .....	144
Terminal interface loopback .....	145
Setting and resetting loopbacks in your local device .....	146
Setting and resetting loopbacks remotely .....	148
Using test codes and BERTs .....	150
Command-line access .....	152
Front-panel access .....	153

## **Chapter 7    Using network management**

Basic network management configuration (Telnet) .....	156
Stand-alone units .....	156
Daisy-chained units, using SLIP .....	156
Daisy-chained units, using Ethernet .....	157
Command-line access .....	158
Front-panel access .....	158
View the current settings .....	159
Setting the IP addresses and netmasks .....	160
Setting the default router IP address .....	163

Setting the Telnet password .....	165
Setting up IP source address screening .....	166
Adding an address to the IP screening list .....	166
Deleting an address from the IP screening list .....	168
Enabling and disabling IP source address screening .....	170
Selecting the IP network interface .....	171
Configuring for SNMP .....	173
Enabling and disabling the SNMP agent .....	173
Setting SNMP community strings .....	174
Configuring the SNMP trap hosts .....	176
Adding an address to the SNMP trap host list .....	176
Deleting an address from the SNMP trap list .....	177
Using SNMP traps .....	179
Configuration for SNMP traps .....	179
Possible types of SNMP traps .....	179
MIB objects included in SNMP traps .....	180
Traps and Alarm Conditions .....	181
MIBs supported by DataSMART MAX .....	182

## **Chapter 8      Quick reference**

Command-line menus and commands .....	184
Front-panel menus and commands .....	191
Commands available via ARC .....	198
DataSMART MAX compatibility .....	199
DataSMART compatibility .....	199
T1 alarms and signal processing .....	200
What happens when alarms occur .....	200
How alarms are generated .....	200
Signal conditions .....	201
Alarms .....	202
Specifications .....	204
<b>Glossary</b> .....	213
<b>Index</b> .....	221





# Preface

---

This manual is the comprehensive reference source for operation of the ADC Kentrox DataSMART MAX T1/FT1 Multimedia Access Multiplexer. It provides specific information for configuring the DataSMART MAX and for using the DataSMART MAX to monitor and troubleshoot the performance of your T1 circuit. It also provides detailed listings of all DataSMART MAX menus, commands, and product specifications.

## Who should read this manual?

This manual is intended as a reference source for ongoing operation of the DataSMART MAX. It covers all possible operations and configuration choices in detail. For initial installation, power up, and basic configuration of the unit, we recommend that you first turn to the *DataSMART MAX T1/FT1 Installation Guide*. Note that installation and service should be performed only by trained and qualified personnel.

## Viewing this manual as a PDF file

This manual is designed to be used as both a printed book and a PDF file, and includes the following features for PDF viewing:

- Cross-references are clickable hyperlinks that appear in blue text.
- Chapters and section headings are represented as clickable bookmarks in the left-hand pane of the Acrobat viewer.
- Page numbering is consistent between the printed page and the PDF file to help you easily select a range of pages for printing.

You can obtain PDF files of our manuals by visiting <http://www.kentrox.com>.

## Related publications

In addition to this manual, the following are available:

- *DataSMART MAX T1/FT1 Installation Guide*  
Detailed procedures for installing the DataSMART MAX hardware and configuring the unit for operation.
- *DataSMART MIB Reference*  
A complete description of traps and tables showing standard and enterprise MIBs for the DataSMART, DataSMART MAX, and DataSMART SPort products.

## MIB source files

MIB source files are available by visiting: <http://www.kentrox.com/support>.

## About this manual

This manual contains the following information:

“Preface” (this section) explains the purpose, organization, and conventions used in this manual and tells how to contact ADC Kentrox Technical Support if you should run into difficulties.

“Introduction” describes the applications and features of the DataSMART MAX. It also introduces you to the DataSMART MAX command-line and front-panel interfaces.

“Establishing system security” shows how to secure the command-line interface and the front-panel interface.

“Configuring the system” describes in detail all of the system-level configuration choices you can make. This includes setting up the system passwords, specifying the system source clock, configuring the alarm formats and output, and configuring the DCE and DTE control ports.

“Configuring interfaces” describes in detail all the configuration choices available for setting up the network interface, the terminal interface in add/drop devices, and the data ports.

“Performance monitoring” shows you how to access and use the DataSMART MAX performance reports and the alarm history report.

“Troubleshooting” shows you how to use the DataSMART MAX to recognize and troubleshoot abnormal conditions in your T1 circuit. It describes use of the DataSMART MAX front-panel LEDs, alarms messages, system status displays, and diagnostic tools such as loopbacks and BERTs.

“Using network management” shows you how to set up and use the DataSMART MAX in an SNMP network management environment. It describes the unit’s embedded SNMP agent and how to establish a Telnet link.

“Quick reference” summarizes DataSMART MAX menus and commands. It includes a complete flowchart of the front-panel LCD interface. It also provides a comprehensive listing of product specifications.

At the back of the manual, you’ll also find a glossary of terms and an index.

## Conventions used in this manual

This manual employs the following conventions when explaining command-line syntax:

<b>Literals</b>	Bold type identifies commands and syntax elements that must be entered exactly as shown in the text.
<i>Variables</i>	Italic type identifies variable syntax elements, such as values or alphanumeric strings you can enter.
<i>x/y</i>	A vertical line between elements means that the elements are mutually exclusive; you can select one and only one of the elements.
[ ]	Brackets indicate items that are optional.

This manual employs the following conventions for the front-panel interface:

<b>SYSTEM STATUS</b> —————→	<b>ALM:-</b> <b>LB:-</b>
FRONT PANEL CFG	<b>NI RX:-</b> <b>TX:-</b>
REPORTS	<b>TI RX:-</b> <b>TX:-</b>
.	<b>DP 1:-</b> <b>2:-</b>
.	<b>DP 3:-</b> <b>4:-</b>
.	

- A vertical line to the left side of a column indicates that you can cycle through the elements in the column by using the Next and Previous push buttons.
- An arrow between elements indicates that you can move between the elements using the Select and Escape push buttons.

## Who to call for assistance

If you need assistance with this product or have questions not answered by this manual, please visit our Support page on the Kentrox Web site. You are also welcome to call or send email to our Technical Assistance Center. Please have your product's software revision and hardware serial numbers available to give to the Support representative. All product returns must include a Return Authorization number, which you can obtain by calling the Technical Assistance Center.

The numbers listed below are current at the time of publication. See the Kentrox Web site for detailed contact and warranty information.

1-800-733-5511 (continental USA only)  
1-503-350-6001  
email: [support@kentrox.com](mailto:support@kentrox.com)  
<http://www.kentrox.com>



## 1

*Introduction*

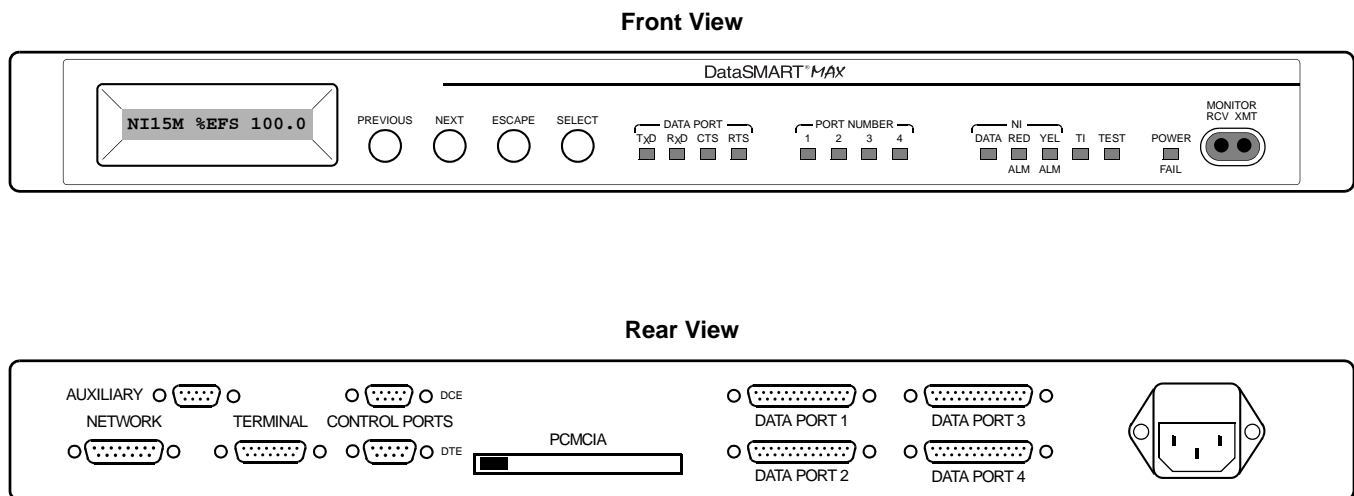
The DataSMART MAX is a Multimedia Access Multiplexer for T1 and fractional T1 lines, providing digital service access for PBX, video/codec, routers, and other customer premise equipment.

The DataSMART MAX comes in two basic configurations with either an AC or DC power supply, for a total of four models. The two basic configurations are:

- The dual-port add/drop model, with two data ports and a terminal interface
- The quad-port add/drop model, with four data ports and a terminal interface

All models are housed in the same one-unit-high (1U) rack-mount box.

**Figure 1—The DataSMART MAX**



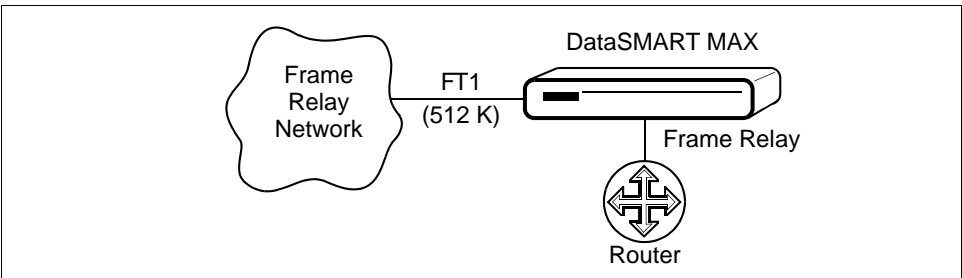
These figures show a quad-port add/drop model. The DataSMART MAX you are working with may not contain some of the LEDs or ports shown here.

# Some examples of applications

The DataSMART MAX supports many applications. Here are three typical setups.

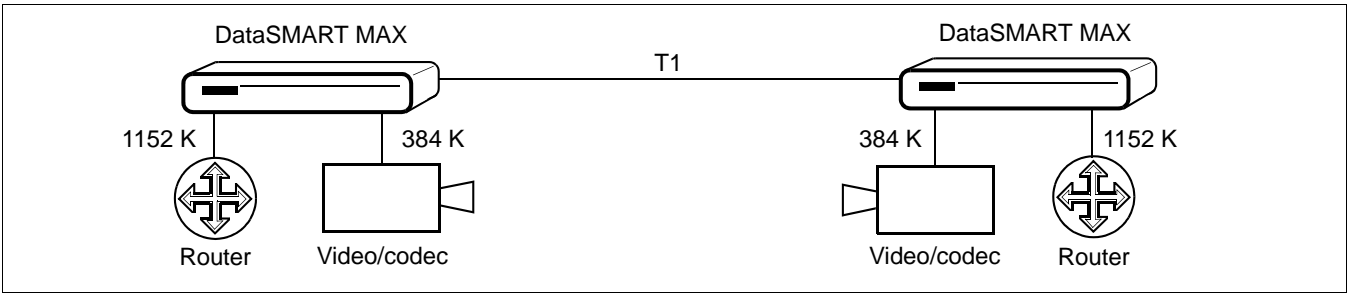
## Fractional T1 and Frame Relay

In this example, the DataSMART MAX DSU/CSU provides connectivity for an enterprise data network. A router sending Frame Relay packets is connected to a data port. The figure shows a DataSMART MAX connected to a fractional T1 line providing 512 kbytes of bandwidth.



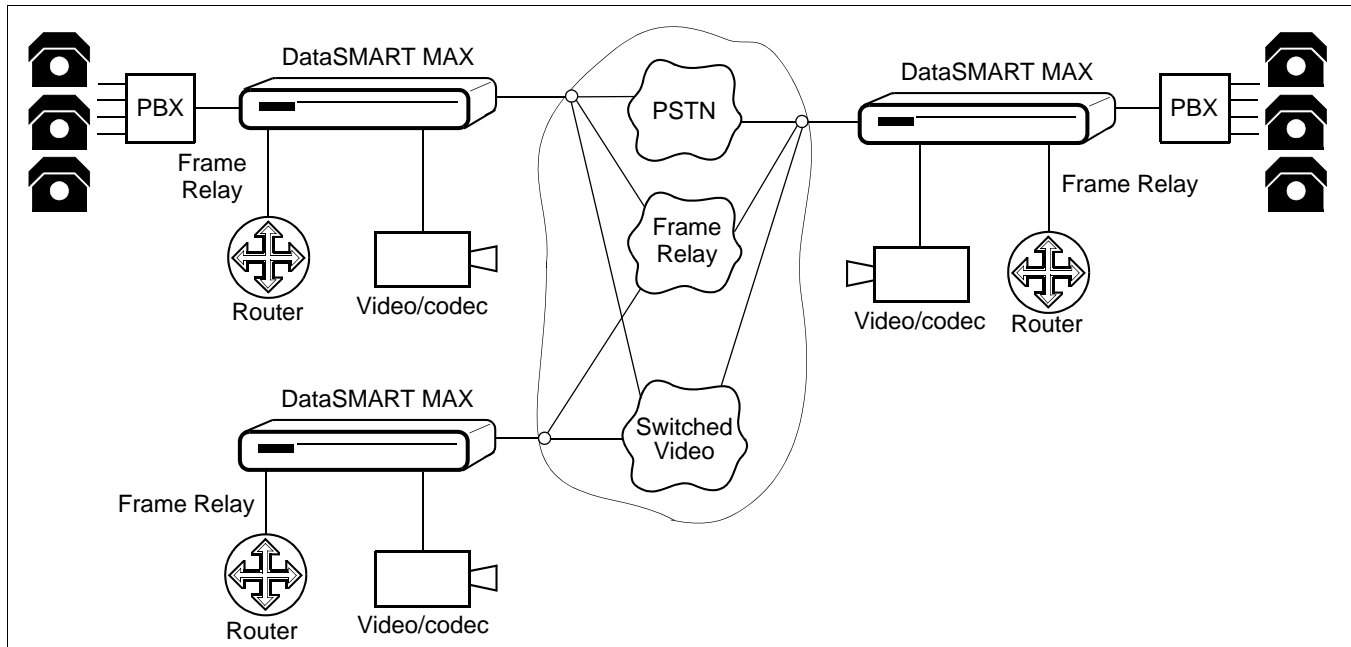
## DSU

Here's another example in which the DataSMART MAX terminates a dedicated T1 facility. A router and a video/codec are connected to the data ports. The network interface is a full T1 line.



## DSU with add/drop

This example shows how DataSMART MAX provides multimedia access multiplexing between several business locations. The PBX connects dial telephones to the public switched telephone network (RTN). The routers connect to a Frame Relay Network and the video/codecs can connect to each other or any video subscriber using switched video service.



---

# Features of the DataSMART MAX Multimedia Access Multiplexer

## A front-panel interface for easy installation

The DataSMART MAX has a front-panel interface that provides command access using an LCD display and four push-buttons. The front-panel interface is modeled after the command-line interface, featuring the full range of functionality as well as a similar structure so that if you know one interface, the other is easy to learn.

The front-panel interface simplifies installation. For instance, if you are planning on managing the DataSMART MAX remotely through SNMP-based network management, the installer does not have to temporarily attach a terminal to complete the installation. Instead the installer can configure the DataSMART MAX using the front panel, then the network manager can complete the setup from the remote station. Of course, the installer could complete the setup from the front panel if desired.

The front-panel interface also simplifies setting up daisy-chained DataSMART MAX units. In this case, even when a terminal is available at the installation site, it is inconvenient to connect it to each DataSMART MAX just to assign the unique address required with daisy-chained units. With the front panel, you have the option of assigning addresses without connecting the terminal.

While the front panel is especially useful for basic setup, you can use it to completely configure a DataSMART MAX. For instance, if it is more convenient for you to assign channels from the front-panel interface (or perhaps modify assignments on a unit that does not have a terminal attached locally), you can do it all from the front-panel.

### Troubleshooting with the front panel

The front panel is a useful tool for monitoring the performance of the T1 lines and troubleshooting. The front-panel System Status display shows the condition of the signal at the network interface, terminal interface, and data ports and reports alarms when they occur. All of the System Status displays are updated dynamically, so as the conditions change on the DataSMART MAX, the display changes.

The front-panel interface is designed so that the System Status information is easily accessible. Just push the Escape button until System Status appears in the display, then push Select, and there you are. The Next or Previous buttons cycle you through the various status displays.

Because the DataSMART MAX allows two people to log in at the same time, the front panel makes it possible for a remote network manager and installer to collaborate during installation. For instance, while the installer performs diagnostics using the front panel, the network manager can watch the progress of the tests.

## All models support all standard data interfaces

On all models of the DataSMART MAX Multimedia Access Multiplexer, the data ports are software programmable. You can configure each data port to use either the V.35 interface or the EIA-530 interface (the EIA-530 interface also supports RS449), so no matter what type of device you have, if there is a port open on the DataSMART MAX, you can connect to it.



## SNMP-based network management

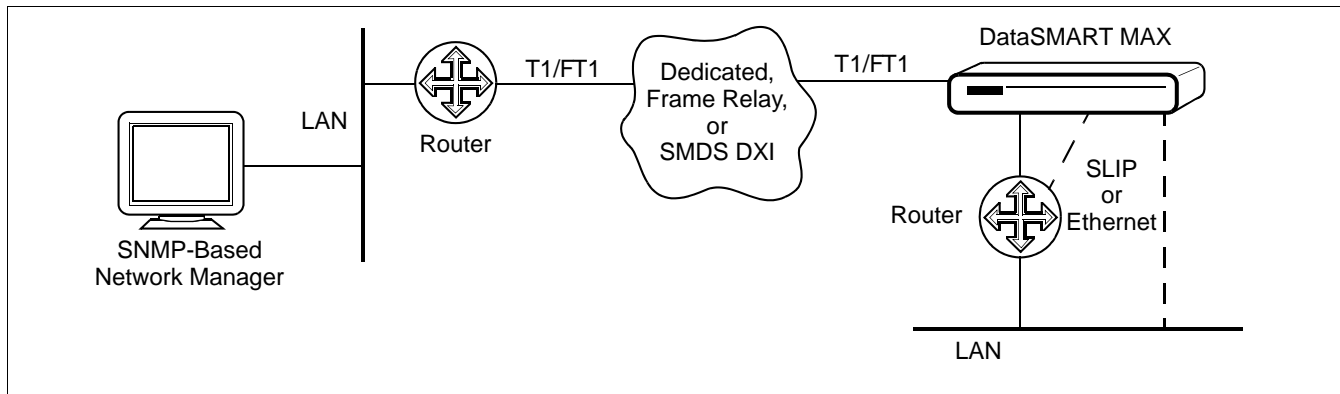
If you are using centralized network management, you can take advantage of the DataSMART MAX's embedded SNMP agent. The SNMP agent allows you to use your network management tool of choice to configure, monitor, and troubleshoot. The SNMP agent also generates traps when network events occur, informing you of abnormal conditions on the T1 line. Additional features of SNMP include pinging and Telnet access to the DataSMART MAX command-line interface.

You have two options for SNMP connectivity. One is through a TCP/IP LAN with an Ethernet connection to the DataSMART MAX (the PCMCIA Ethernet interface is an accessory on the DataSMART MAX). The other is through a SLIP-capable device, such as a router, connected to the DataSMART MAX control port.

With either option, the SNMP link between the network management application and the DataSMART MAX is in-band, using the existing T1 line instead of costly dial-up lines (see the figure below).

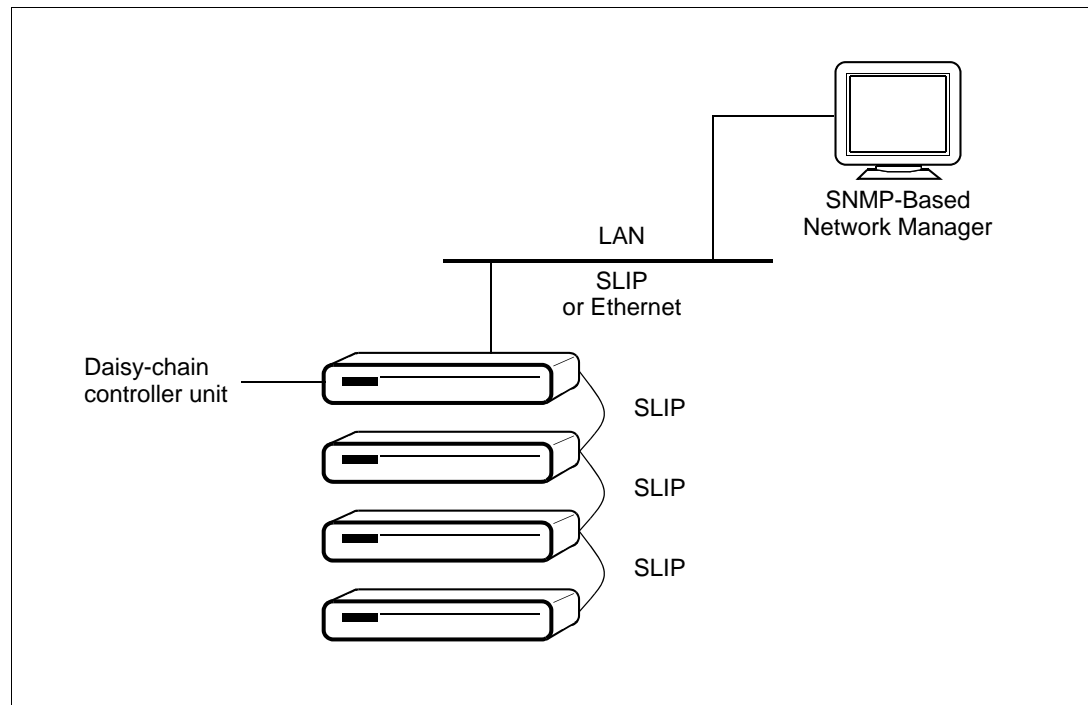
The SNMP agent supports MIB II (which facilitates the management of a LAN-based host, in this case, the DataSMART MAX) and the DS1 MIB (which facilitates the management of a T1 line.)

We also provide an Enterprise MIB which allows complete management of the DataSMART MAX, supporting via SNMP everything that is available through the control port menu interface.



## Daisy-chain control: SLIP or Ethernet

You can control daisy-chained units via a SLIP or Ethernet connection. The first unit in the connection acts as the daisy-chain controller. It connects to the network management system via Ethernet or SLIP. The other units in the chain are connected to the controller unit via their control ports and are set up for SLIP access only. The controller acts like a “gateway” or “router” between the Ethernet LAN and the other daisy-chained units.



## Facility data link

The DataSMART MAX supports a facility data link (FDL) when configured for Extended Super Frame (ESF). The FDL is a bidirectional 4 Kbps data line within the T1 bit stream. The FDL supports the following:

- Exchange of performance data, so a DataSMART MAX can get a complete picture of the performance of the T1 line at the network interface of a far-end unit
- A communication link the carrier can use to query the DataSMART MAX about the status and performance of the network line
- Remote login between DataSMART MAX units
- Using a DataSMART MAX to configure data ports and collect status information on a remote DataSMART

## T1 performance monitoring

The DataSMART MAX has extensive non-intrusive reports that show the performance of the T1 lines at the network interface and terminal interface. With these reports you can see the quality of the signal over a period of time and recognize problems before the service goes down. If the DataSMART MAX loses power, all performance data is guaranteed to be retained for two hours.

The performance monitoring reports show the signal quality for the previous 24 hours in 15-minute increments and the signal quality for the last seven days in 24-hour increments. For the network interface reports, the DataSMART MAX maintains separate registers for both the user (the T1 customer) and the carrier.

All reports are detailed, including information on various types of error counts and alarm states. They are easy to read and can be formatted for printable files or screen display. A subset of the information in the reports is also available for viewing in the front-panel LCD.

## **T1 diagnostics**

The DataSMART MAX offers a complete suite of diagnostic tools, including:

- LEDs for alerting you to problems on lines at the network interface, data ports, and terminal interface
- Alarm messages and SNMP traps
- Loopbacks that can be set remotely or locally
- Test code generator that generates QRS, 3 in 24, all 1s, or all 0s (for testing the full T1 line), or that generates 511 and 2047 (for testing just the channels assigned to a specific data port)
- Bit error rate testing (BERT), for monitoring the received test codes

## **Nonvolatile memory**

The DataSMART MAX configuration is stored in nonvolatile memory, so the DataSMART MAX can retain its configuration for a minimum of ten years without power.

---

# Using the DataSMART MAX

## Using the command-line interface

With the command-line interface you use a terminal to manage and monitor the DataSMART MAX.

To help you find your way through the interface, the DataSMART MAX uses “menus” that might be more properly thought of as help displays.

Each command is categorized and placed in a menu. For instance, all the commands for generating reports are in the Reports menu. To see the list of all menus as shown in the following figure, enter **MM**.

**Figure 2—The Main menu**

```
DataSMART MAX T1 4 Port A/D Ver. 1.31 Copyright (c) 1995-96 Kentrox
ADDRESS: 00:00:000 NAME: PORTLAND,OR

MM          - Main Menu
SS          - System Status and Remote Menu
R           - Reports Menu

LM          - Local Maintenance Menu
RM          - Remote Maintenance Menu

AC          - Alarm Configuration Menu
CC          - Control Port Configuration Menu
DC          - Data Port Configuration Menu
FC          - Fractional T1 Configuration Menu
MC          - Management Configuration Menu
NC          - NI Configuration Menu
PC          - Password Entry and Configuration Menu
SC          - System Configuration Menu
TC          - TI Configuration Menu

^D          - Logout
^D<xx>:<yy>:<zzz>^E - Address Another Unit

MM>
```

To see one of the menus, enter the menu name at the prompt. For instance, to see the Reports menu, enter **R** at the prompt.

```
MM> R

REPORTS MENU

UNSR / UNLR - User NI Short/Long Performance Report
UTSR / UTLR - User TI Short/Long Performance Report
CNSR / CNLR - Carrier NI Short/Long Performance Report
FESR / FELR - Far End PRM Short/Long Performance Report

NSR:[z]     - User NI Statistical Performance Report
TSR:[z]     - User TI Statistical Performance Report
             z = Display Report then Zero Counts (Optional)
AHR         - Alarm History Report

PL:<len|style> - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
               <style> = P (Page Break), M (More), or V (View)

R>
```

Each time you change menus the command-line prompt changes to indicate which menu is current. In the preceding figure, the first line shows a prompt of “MM>” meaning that the Main menu is current. However, once R is entered and the Reports menu is displayed, the prompt becomes “R>,” indicating that the Reports menu is current.

The current menu displays when you press the Enter key. In normal use you are likely to use a series of commands from a given menu, and so you can make that menu current and get a menu listing whenever you need it by pressing the Enter key. However, you may enter any command at the command line, even if it is not on the “current” menu.

### Command-line syntax

A typical command line consists of the command and zero or more arguments, all separated by one or more delimiters. The following are all valid delimiters: a space, a tab, a comma, a colon, a forward slash.

For example, the following are all valid commands to set the date to December 8, 1995:

**SD:12:08:95**

**SD 12/08/95**

**SD 12 08 95**

**SD::12::08::95**

There are two exceptions to these rules. One is the **SN** command, used for assigning a site name. In this case, a space, comma, forward slash, or colon can appear in the argument, as long as there is a non-delimiter preceding it (not necessarily immediately preceding it). For example, this is a valid instance of the **SN** command:

**SN PORTLAND, OR**

The other exception is the syntax for logging into daisy-chained DataSMART MAX units (see [“Logging in” on page 26](#)).

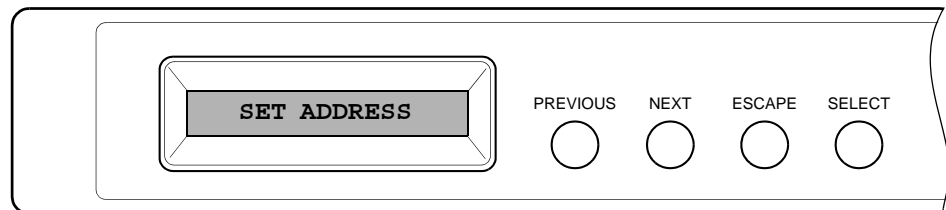
### Type-ahead

You may enter the next command while a previous command is executing. The maximum type-ahead is three commands or 256 characters, whichever is less.

## Using the front-panel interface

The front-panel interface is modeled after the command-line interface and provides most of the same functionality. The front-panel interface uses a hierarchical structure that you traverse using four push-buttons on the front panel to find the command you need. The LCD display provides the visual readout.

**Figure 3—The LCD display and push-buttons**



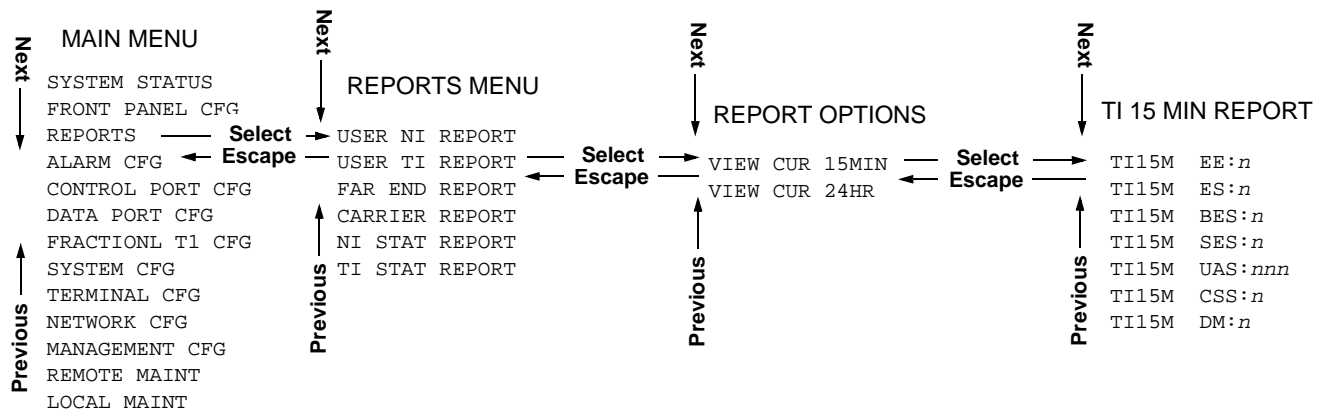
The hierarchical levels of the front-panel interface correspond to the menus, commands, and command options of the command-line interface. The Main menu at the top of the hierarchy corresponds to the Main menu of the command-line interface. Below that, depending on the complexity of the command, submenus correspond to the command menus of the command-line interface, then further subtrees allow you to select command options.

## Traversing the hierarchy

The Select button moves you deeper into the hierarchy, the Escape button moves you back out towards the top. Next or Previous cycles you through all elements in one level of the hierarchy.

The figure below illustrates these rules.

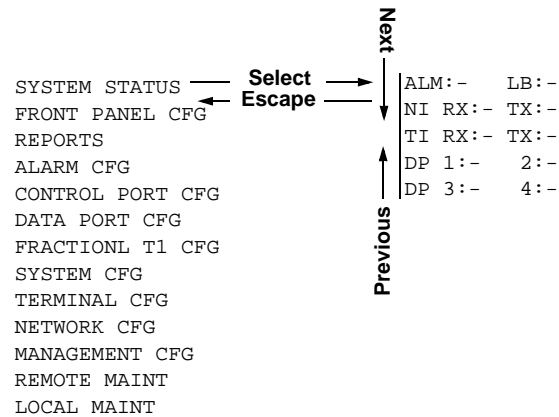
- 1 The Main menu is on the left side of the figure. Push Next or Previous to cycle through the items on the Main menu. When you see the item you want, push Select to descend to the next level, in this case the Reports menu.
- 2 In the Reports menu, push Next or Previous to cycle through the report choices. When you see the report you want, push Select to descend to the next level, the Report Options.
- 3 From the Report Options menu, choose to view either the report for the current 15 minutes or the current 24 hours; then push Select to descend to the first item in the report display.
- 4 As shown in the figure, the report display contains seven items that you can cycle through using Next or Previous.



Notice that you can “cycle” through items at each level in the hierarchy, and yet there is a conceptual “top” to each. Each level is circular in that pushing Next or Previous eventually brings you back to where you started. Each level has a “top” in that whenever you descend to a level by pushing Select, you always see the top item in the level. In the case of the Reports menu, the top item is USER NI REPORT.

However, when you use Escape to ascend from one level to the one above, you go back to the item that you originally descended from. For instance, if you entered the Report Options menu from USER TI REPORT, you would return to USER TI REPORT if you pushed Escape.

Not all hierarchies in the front-panel interface are as complex as the one in the last example. For instance, the simplest is for reading the System Status. In this case, when you see SYSTEM STATUS in the display, push Select. You can then use Next or Previous to cycle through the System Status display.



### NOTE

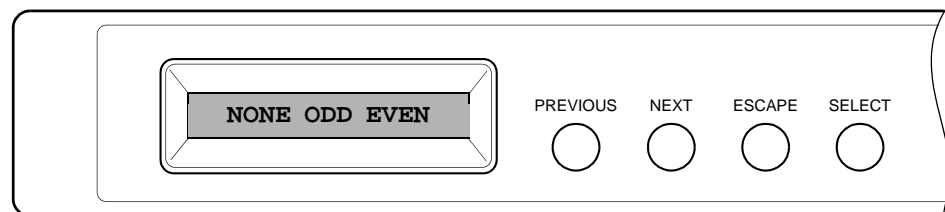
*If you lose your place in the hierarchy, you can always return to a known point by pushing the Escape button until you see SYSTEM STATUS in the display; you will be back at the top of the Main menu.*

### Using the front panel for entering values

You can use the front panel for configuring ports, channels, and performing other operations that require you to enter values. There are three basic situations when entering values:

- selecting from multiple choices displayed together in the panel
- selecting multiple choices by cycling through a list
- entering a string, IP address, or channel configuration

**Selecting from multiple choices displayed together.** The figure below illustrates choices displayed together, in this case the parity setting for the control port.



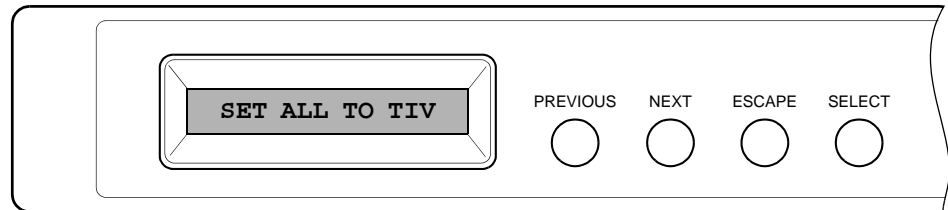
When the display appears, the current selection is blinking. To change to another value in the display, push Next or Previous. As you cycle through the selections, each will blink in turn.

**TIP**

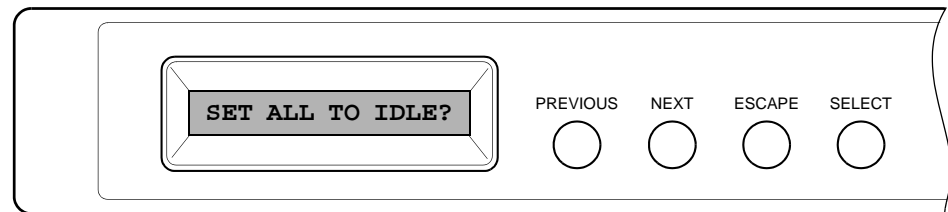
*When you change a setting in the LCD display, a question mark appears indicating that a change to the DataSMART MAX configuration is pending. Push Select to change to the configuration; push Escape to return the display to the original setting with no change to the configuration.*

As soon as you change a selection in the display, a question mark appears on the right side of the display, indicating a change has been made in the display that has not yet been made to the DataSMART MAX configuration. Push Select to make the change to the configuration and the question mark disappears (except in the case of entering a string, IP address, or channel configuration. See heading after next.)

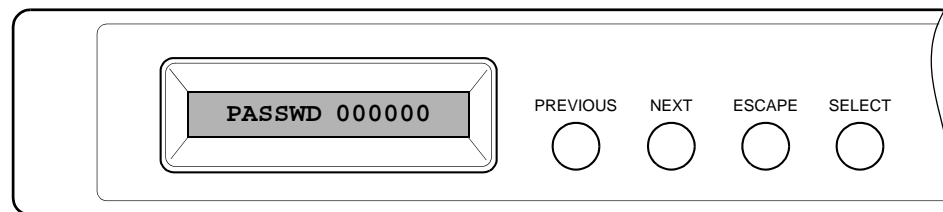
**Selecting multiple choices by cycling through a list.** In this case, you cannot see all your choices in the display. For example, the following figure shows a display for fractional T1 configuration. In the display “TIV” blinks to indicate that it is the current selection and can be changed.



Pushing Next changes the selection to “IDLE” as shown below. The question mark indicates that a change to the configuration is pending. If you push Select now, IDLE will become the current configuration.



**Entering a string, IP address, or channel configuration.** The figure below illustrates the display for changing the front-panel password. As the figure shows, a password is a string of six numerals.

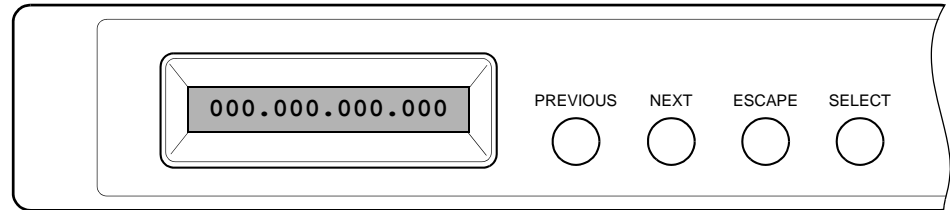


When the display first comes up, the first numeral is underlined. Pushing Next or Previous moves the underline to a different numeral. To change the underlined numeral, push Select. The underline disappears and the numeral begins blinking. When the numeral is blinking, push Next or Previous to change the numeral.

As soon as you change the numeral in the display, a question mark appears to the right, indicating that you have changed a value in the display but have not yet changed the value in the DataSMART MAX configuration. Push Select to make the change to the configuration. The numeral stops blinking, the question mark disappears, and the underline reappears. You can now use Next or Previous to move the underline to a different numeral for further editing. If you push Escape when the question mark is showing, the numeral returns to its original setting.



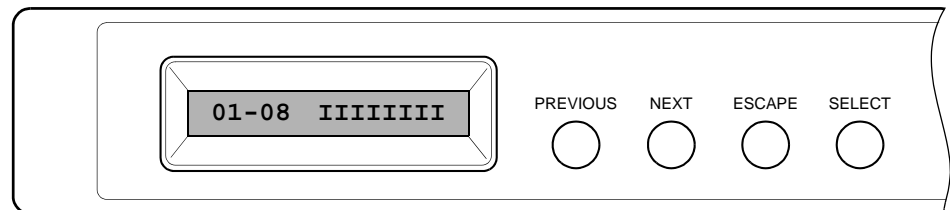
Entering an address works similarly, though with some differences worth noting. For instance, the following figure shows the display for setting the IP address. In this case, Next or Previous moves the underline between the fields rather than stopping at each numeral. You use the same procedure to change the fields as for changing the numerals of a password.



The question mark appears each time you edit a field, and disappears when you push Select. However, the changes you make in the display do not take effect in the DataSMART MAX configuration until you leave the IP address display. In other words, after you make all the changes to the fields (pushing Select after each one), you must push Escape. The query SET NEW ADDRESS? appears in the display. If you push Select, the changes are made to the configuration. If you push Escape, the changes you made in the display are discarded.

The process for entering channel configurations has similarities to both entering strings and entering addresses.

The following figure shows the initial channel configuration display. The display shows the settings for channels one through eight, which in this case are all set to idle, as indicated by an “I” for each channel.



When you first enter the display, the channel range is blinking. If you push Next or Previous at this point, the ranges will cycle through “01- 08”, “09-16”, and “17 - 24.” When you see the range you want to edit, push Select. The range will stop blinking, and an underline will appear under the token representing the first channel.

At this point, you change the token just as you would change a numeral in the password string. Push Select, and the token begins blinking, then push Next or Previous to change the token. The question mark appears when you change the token. When you have changed the token to the one you want, push Select; the question mark disappears and the underline reappears. You can then use Next or Previous to move the underline to the next token you wish to change.

Once all the channels for the range are correctly set, push Escape. The range begins blinking and you can change to the next range. When all the channels are set correctly, push Escape to exit the channel configuration display. The query “LOAD NEW CHANS?” appears. Push Select to load the new channel configuration into the hardware or push Escape to discard the changes.

---

## Logging in

In general, a password is not needed to log into a DataSMART MAX. Though the DataSMART MAX supports passwords, the passwords do not prevent login but instead restrict users from executing various commands. (See Chapter 2 for procedures on setting passwords.)

Depending on whether you are accessing the DataSMART MAX through Telnet, the facility data link, or a control port, and on whether the DataSMART MAX is daisy-chained or is stand-alone, the procedure for logging in differs.

### Through the control port: stand-alone

On a stand-alone unit, the device typically has the address of 00:00:000. In this case, simply push the Enter key to log in. The DataSMART MAX will display the Main menu, and then the command prompt, indicating you are logged in.

### Through the control port: daisy-chained

With daisy-chained units, each unit in the daisy chain has an address. To log into a DataSMART MAX that is daisy-chained, enter this:

`<Ctrl-D>xx:yy:zzz<Ctrl-E>`

where `xx:yy:zzz` is the address of the unit you want to log into. Note that the colon is the only valid delimiter for the login command.

### Through the FDL

The facility data link uses a signal embedded in the T1 framing pattern to enable you to log into a far-end DataSMART MAX or DataSMART. You must be logged into the near-end DataSMART MAX to use this method. Once you are logged into the near-end DataSMART MAX, enter this command:

**ARC**

The angle brackets in the command prompt will change from “>” to “<” to indicate that you are logged into a far-end unit.

You log out of the far-end unit by entering this command:

**DRC**

### Telnet access

You can log into the DataSMART MAX using Telnet. When you attempt to log in, you will be prompted for a Telnet password. You must assign a Telnet password to the DataSMART MAX before you attempt to access it via Telnet. If the DataSMART MAX has not been assigned a Telnet password, you will not be able to log in.

Note that when you are logged into a DataSMART MAX using Telnet, you cannot use the **ARC** command to log into another DataSMART MAX. Instead, log out and then Telnet directly to the desired DataSMART MAX.

See Chapter 7 for information on configuring a DataSMART MAX for Telnet login.

### Front panel

By default, the front panel is enabled and accessible to anyone; no login is required. You can restrict access to the front panel by establishing a password (see Chapter 2), then disabling access. The next user must then enter the password to enable the front panel.

## Logging out

You should always log out of the DataSMART MAX when you are done.

To log out, enter <Ctrl-D>.

If you have logged into a remote DataSMART MAX using **ARC**, use the **DRC** command or <Ctrl-D> to log out.

You can also log out by disconnecting the control port cable.

The DataSMART MAX has an auto-logout feature, that will log you out after a period of inactivity. (See pages [48](#) and [49](#).)



# 2

## *Establishing system security*

---

The DataSMART MAX can be accessed through an SNMP network manager, through the command-line interface using either a terminal or Telnet, or through the front-panel interface. In order to prevent unauthorized users from changing the system configuration, setting loop-backs, or performing other operations that might disrupt service, you must secure each of these interfaces.

This chapter covers the following topics:

- Securing the command-line interface
- Securing the front-panel interface

For information about securing SNMP access with community strings, refer to Chapter 7, “[Setting SNMP community strings](#)”, on page 174.

---

# Securing the command-line interface

Security for the command-line interface is achieved through a system of passwords and privilege levels. Any user can access the command line without entering a password. But in order to gain a specific privilege level, the user must enter a password that has that privilege level assigned to it.

By default, there are no restrictions on which commands you can run on the DataSMART MAX. Every user has super-user privileges. In order to restrict access, you must create at least one password with the super-user privilege level. Once you do, every user is restricted to the read-only privilege level unless they enter a password that permits more extensive privileges. You may create up to ten passwords (assuming you have super-user privileges) and assign them any privilege level you like.



**NOTE**

*If you do not create a password with a super-user privilege level, every user that accesses the command line will be granted super-user privileges, regardless of whether or not you have created passwords for the other privilege levels.*

**Table 1—Privilege levels**

Privilege level	Description
Read-only	Users with no password, and thus no privilege level, have read-only access. They can view menus, status screens, and performance reports, but they cannot execute any diagnostics nor change any configuration options.
Maintenance	Users with this privilege level can execute diagnostic tests, such as loopbacks and BERTs. Their activities can potentially disrupt data traffic through the device.
Configuration	Users with this privilege level can execute all tests allowed at the Maintenance level, plus they can change the configuration options of the DataSMART MAX. Their activities can potentially disrupt service to the device.
Super user	Users with this privilege level have access to all commands allowed at the Configuration level, plus they have access to the commands that set up and control passwords.

**Using Telnet**

If you are using Telnet, you must set up a Telnet password, which is independent of the command-line passwords described here. See [“Setting the Telnet password” on page 165](#).

The commands available for setting up and controlling command-line passwords are listed in the Password Entry and Configuration menu. To display this menu, enter **PC** at the command line.

#### PASSWORD ENTRY AND CONFIGURATION MENU

```
EPS:<password>          - Enter Password
                        password = 6 to 12 characters

APS:<access>:<password> - Add Password
                        access  = SA - Super User
                                CA - Configuration
                                MA - Maintenance
                        password = 6 to 12 characters

DPS:<password>          - Delete Password
                        password = 6 to 12 characters, or * for all

PUV                      - View User Access Privilege
PCV                      - View Password Configuration
```

Passwords are stored in the permanent nonvolatile configuration database.

## Adding a password

You create a new password by using the **APS** command. You must have super-user privileges. The command syntax is:

**APS:***access:password*

*access* Specify the privilege level you want linked to the password: **SA** (super user), **CA** (configuration), or **MA** (maintenance).

*password* Specify the password you want added. The string can comprise from six to twelve ASCII printable characters. Passwords are not case-sensitive and trailing spaces are not truncated.

Up to ten passwords are allowed. If you attempt to enter an eleventh password, you will receive an error message. To add another password, you must first delete an existing password.

Each password must be unique.

## Deleting a password

You delete a password using the **DPS** command. You must have super-user privileges. The command syntax is:

**DPS:***password*

*password* Specify the password you want deleted. The string must match the password exactly, except for case. You can also enter the \* wild-card character to delete all current passwords.

## Entering a password

To gain the privilege level associated with a password, use the **EPS** command. No special privileges are required. The command syntax is:

**EPS:***password*

*password*                      Enter the password. Passwords are not case-sensitive.

If you enter the password correctly, DataSMART MAX responds with the message **PASSWORD ACCEPTED**. If you enter an incorrect password, it responds with the message **PASSWORD DENIED**.

## Viewing a user's access level

If you are logged into the device, you can view your privilege level by using the **PUV** command. You do not need any special privilege level. You will receive one of the following messages:

- “User has No Access Privileges”
- “User has MA Access Privileges” (maintenance)
- “User has CA Access Privileges” (configuration)
- “User has SA Access Privileges” (super user)

If your password was modified during your current session (e.g., a super user deleted your password, then added it back with a different privilege level), the change will not become effective until the next time you specify the password with the **EPS** command.

## Viewing the current passwords

You can view a listing of current passwords and their privilege levels using the **PCV** command. You must have super-user privileges.

An example listing is shown below. The left column lists the current passwords, the right column identifies the access privilege levels.

VIEW PASSWORD CONFIGURATION	
Password	Access
-----	-----
BROWNS	MA
JOHNSOND	CA
MITCHELLS	SA



---

## Securing the front panel

After you have installed the DataSMART MAX and are controlling it remotely, you may want to disable the front-panel LCD and keypad controls. Disabling the front panel prevents unauthorized or careless users from changing the DataSMART MAX configuration and disrupting service.

A disabled front panel can be used for examining status, performance, and configuration, but not for changing any parameters. One way to think of it is that a disabled front panel is in “read-only mode” while an enabled front panel is in “read/write mode.”



### NOTE

*The only configuration value that the user can change from a disabled front panel is the setting for the data port LEDs (using the SET DP LEDS option). This cycles the data port LED readout between the various data ports.*

There are two approaches to disabling the front panel. You can disable the front panel without setting a front-panel password, or you can set a password and disable it.

If you do not set a password, any user can disable, then re-enable the front panel. This provides minimum security for times when you want to temporarily disable configuration access. For example, you might want to secure the front panel this way while you are viewing status, since this would prevent you from inadvertently changing a parameter while pushing buttons. However, for full security, you want to set a password. If you set a password, only users who enter the password can re-enable the front panel once it has been disabled. The front panel can also be re-enabled by entering **EFP** from the control port.

### Using auto-logout

Another benefit to setting a front-panel password is that you can employ the front-panel auto-logout feature. This feature automatically disables the front panel if there has been no user activity at the front panel for a specified period of time. The front-panel display switches to a readout of %EFS (percentage error-free seconds) when the auto-logout occurs. The next user needs to enter the password to re-enable the front panel.

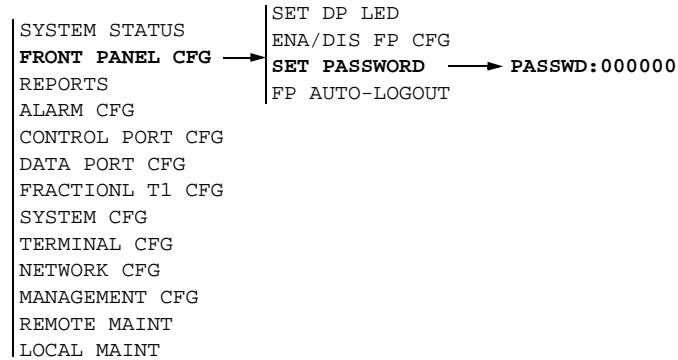
If a password has not been defined for the front panel, the auto-logout feature has no effect except to show the %EFS display.

## Setting the front-panel password

To set the front-panel password, use the steps shown below. The password is six digits. All zeroes is the equivalent of “no password.” Note that if the front panel is disabled, instead of seeing SET PASSWORD in the display, you will see ENTER PASSWORD.

The default password is 000000 (no password).

The password is stored in the permanent nonvolatile configuration database.

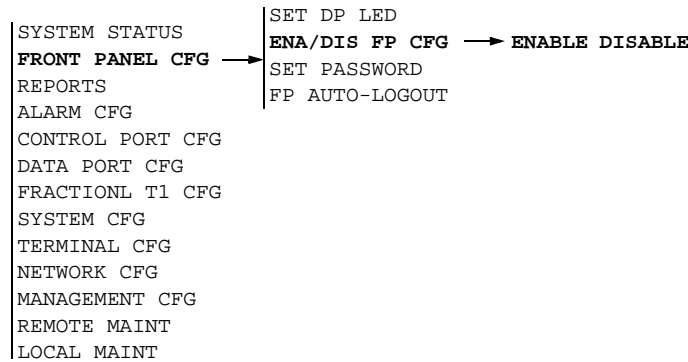


- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRONT PANEL CFG appears in the display.
- 3 Push Select. SET DP LED appears in the display.
- 4 Push Next or Previous until SET PASSWORD appears in the display.
- 5 Push Select. PASSWD:000000 appears in the display.
- 6 Push Next or Previous to move the underline marker to the digit field you want to change.
- 7 Push Select. The digit will blink.
- 8 Use Next or Previous to change the digit value.
- 9 When the digit is set to the value you want, push Select. The message PASSWD SET indicates that the password has been changed.
- 10 Repeat steps 6 through 9 to change the rest of the digits as desired.

## Enabling/disabling the front panel

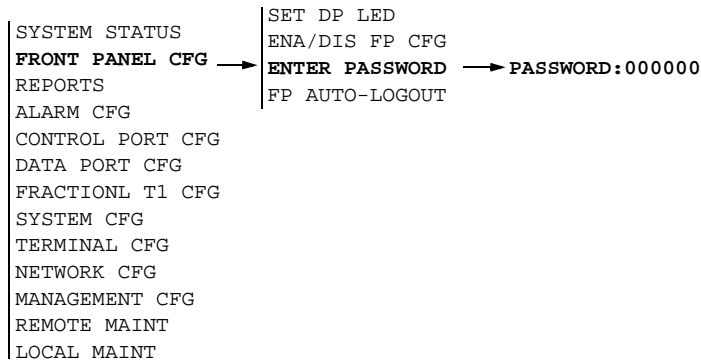
The default state for the front panel is enabled. The setting is stored in the permanent nonvolatile configuration database.

To enable or disable the front panel when no password is set, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRONT PANEL CFG appears in the display.
- 3 Push Select. SET DP LED appears in the display.
- 4 Push Next or Previous until ENA/DIS FP CFG appears in the display.
- 5 Push Select. ENABLE DISABLE appears in the display, with the current selection blinking.
- 6 Push Next or Previous to choose the desired selection.
- 7 Push Select.

To enable the front panel when a password is set, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRONT PANEL CFG appears in the display.
- 3 Push Select. SET DP LED appears in the display.
- 4 Push Next or Previous until ENTER PASSWORD appears in the display.
- 5 Push Select. PASSWD:000000 appears in the display.
- 6 Push Next or Previous to move the underline marker to the appropriate digit field.

- 7 Push Select. The digit will blink.
- 8 Use Next or Previous to specify the appropriate digit.
- 9 Push Select.
- 10 Repeat steps 6 through 9 to change the rest of the digits to the correct password.  
When the password is correct, **PASSWD ACCEPTED** appears in the display.

### Using the command line

You can also enable or disable the front panel from the command-line interface by using the **EFP** and **DFP** commands, respectively. You must have super-user or configuration privileges.

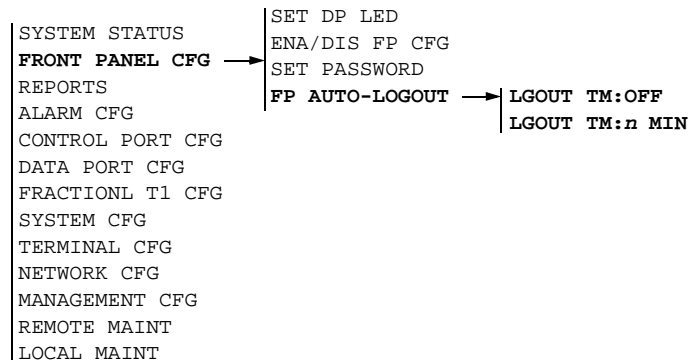
**EFP** Enable the front panel.  
**DFP** Disable the front panel.

## Setting auto-logout for the front panel

You can set the auto-logout timer to OFF (disabled), or from 1 to 60 minutes, inclusive. Use the steps shown below.

The default for auto-logout is OFF.

The auto-logout setting is stored in the permanent nonvolatile configuration database.



- 1 Push Escape until **SYSTEM STATUS** appears in the display.
- 2 Push Next or Previous until **FRONT PANEL CFG** appears in the display.
- 3 Push Select. **SET DP LED** appears in the display.
- 4 Push Next or Previous until **FP AUTO-LOGOUT** appears in the display.
- 5 Push Select. The current auto-logout setting appears: OFF or a value from 1 to 60.
- 6 Push Next or Previous to change the timer value, then push Select.

## 3

*Configuring the system*

---

This chapter discusses configuration operations that apply to the DataSMART MAX as a whole. It covers the commands and options listed in the System Configuration, Control Port Configuration, and Alarm Configuration menus.

Topics include:

- Setting the DataSMART MAX real-time clock and source clock
- Resetting the device to its default state
- Configuring the control port
- Configuring alarm message output and format

For information on configuring interface ports and assigning channels, see Chapter 4.

For information on configuring the DataSMART MAX for network management, see Chapter 7.

---

# Specifying system parameters

You can control the system-level parameters and activities by using the command-line interface or the front-panel interface.

## Command-line access

The commands for configuring the system parameters are listed below (enter **SC** to see this display).

SYSTEM CONFIGURATION MENU	
SD:<mm>,<dd>,<yy>	- Set Date (Warning: This also clears reports)
ST:<hh>,<mm>	- Set Time (Warning: This also clears reports)
SN:<id>	- Set Name
SA:<xx>,<yy>,<zzz>	- Set the Unit's Address to slot:shelf:group
EFP / DFP	- Enable/Disable Front Panel Operation
EDC / DDC	- Enable/Disable DataSMART compatibility
CLK:<src>	- Clock Source, src = L (Loop), T (TI Receive), I (Internal), E (External), <n> (Data Port at n=1..4)
ALGOUT:<n>	- Autologout, n = 0 .. 60 minutes
ZALL	- Zero All Counters used in User Reports
MCSWDL	- Download program from memory card
WYV	- View "What's Your Version" Information
RSD	- Reset System to Default Values
SCV	- View System Configuration

## Front-panel access

The front-panel commands for configuring the system are as follows.

SYSTEM STATUS	
FRONT PANEL CFG	
REPORTS	
ALARM CFG	
CONTROL PORT CFG	
DATA PORT CFG	
FRACTIONL T1 CFG	
<b>SYSTEM CFG</b> →	<b>SET DATE</b>
TERMINAL CFG	<b>SET TIME</b>
NETWORK CFG	<b>SET NAME</b>
MANAGEMENT CFG	<b>SET ADDRESS</b>
REMOTE MAINT	<b>DATASmart COMPAT</b>
LOCAL MAINT	<b>CLOCK SOURCE</b>
	<b>AUTO-LOGOUT TIME</b>
	<b>ZERO COUNTERS</b>
	<b>DOWNLD CARD PROG</b>
	<b>VERSION INFO</b>
	<b>RESET DEFAULTS</b>

## Viewing the current settings

Before changing any system parameters, you may want to look at the current settings. You do this by executing the **SCV** command. This command displays the View System Configuration screen.

```
VIEW SYSTEM CONFIGURATION

Date           Time      Name           Address        Autologout
-----
JAN  7, 1995   21:37  PORTLAND,OR    00:00:000     DISABLED

User Clock     Current Clock  Front Panel    Compatibility
-----
LOOP           LOOP           ENABLED        DATASSMART MAX
```

Field	Description
Date	This field displays the current date of the real-time clock.
Time	This field displays the current time of the real-time clock.
Name	This field displays the name of the DataSMART MAX you are logged into. The name appears in the Main menu, in all performance reports, and in alarm messages. It is also the name returned for the MIB II <i>sysName</i> object.
Address	This field displays the address of the DataSMART MAX you are logged into. This is not the internet address, but is the address assigned for the purposes of distinguishing between daisy-chained DataSMART MAX units.
Autologout	This field specifies the state of auto-logout. If auto-logout is enabled, it displays the auto-logout period in minutes.
User Clock	This field identifies the clock source that you have assigned to be used as the system clock.
Current Clock	This field tells you the <i>actual</i> clock source being used as the system clock. In most circumstances, this field will be identical to the "User Clock." It will differ from "User Clock" if the DataSMART MAX has lost its primary clock source.
Front Panel	This field tells you if the front panel is currently enabled or disabled.
Compatibility (ARC Mode)	This field tells you if ARC mode is set for compatibility with a DataSMART MAX or a DataSMART (see <a href="#">page 198</a> ).

# Setting date and time

DataSMART MAX uses its internal, real-time clock to time stamp event occurrences. The time stamps appear in alarm messages and performance reports as an aid to troubleshooting. To make the time stamps meaningful, you must set the date and time of the real-time clock upon system installation.

Once you have set the real-time clock, you need to reset it only if the DataSMART MAX has an extended power loss. The real-time clock operates for ten hours, nominally, after power is lost.



## CAUTION!

When you change the date or time parameters of the real-time clock, all performance data is cleared from the performance reports.

## Using the command line

You set the date by using the **SD** command. You must have super-user or configuration privileges. The command syntax is:

**SD:mm,dd,yy**

- |           |  |
|-----------|--|
| <i>mm</i> | Specify the month. You can enter the three-letter abbreviation or the number of the month.   |
| <i>dd</i> | Specify the day of the month. DataSMART MAX performs a range check on the entered value to see if the day is valid for the given month and year. |
| <i>yy</i> | Specify the last two digits of the year.   |

### TIP

*If you want to track between Daylight Savings Time and Standard Time, you will need to reset the “time” parameter as appropriate.*

You set the time by using the **ST** command. You must have super-user or configuration privileges. The command syntax is:

**ST:hh,mm**

- |           |  |
|-----------|--|
| <i>hh</i> | Specify the hour. The time is specified in “24-hour” format, where 12:00 is noon and 00:00 is midnight. Allowed values are 0 to 23, inclusive. |
| <i>mm</i> | Specify the minutes. Allowed values are 0 to 59, inclusive.  |



## Using the front panel

To set the date and time from the front panel, use these steps.

SYSTEM STATUS	
FRONT PANEL CFG	
REPORTS	
ALARM CFG	
CONTROL PORT CFG	
DATA PORT CFG	
FRACTIONL T1 CFG	
<b>SYSTEM CFG</b> →	<b>SET DATE</b> → <i>mmm dd,yyyy</i>
TERMINAL CFG	<b>SET TIME</b> → <i>hh:mm</i>
NETWORK CFG	SET NAME
MANAGEMENT CFG	SET ADDRESS
REMOTE MAINT	DATASmart COMPAT
LOCAL MAINT	CLOCK SOURCE
	AUTO-LOGOUT TIME
	ZERO COUNTERS
	DOWNLD CARD PROG
	VERSION INFO
	RESET DEFAULTS

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display.
- 3 Push Select. SET DATE appears in the display.
- 4 If you want to change the date, push Select. A string showing the date appears in the display.  
  
If you want to change the time, push Next or Previous until SET TIME appears in the display, then push Select. A string showing the current time appears in the display.
- 5 The SET DATE and SET TIME strings are divided into fields. To select a field to change, push Next or Previous until the field is underlined, then push Select.
- 6 Push Next or Previous to cycle through the allowed field values.
- 7 When the value you want is displayed, push Select. The LCD displays CLR PERF DATA? to remind you that changing the date or time clears performance data from the performance reports. Push Select again to change the date or time, or push Escape to abort. If you push Select, PERF DATA CLEARD appears on the screen, indicating that the date or time has been reset and the performance data cleared.
- 8 Repeat steps 4 through 7 to change each field in the date or time string.

# Naming the device

Each DataSMART MAX is assigned a device name that appears in alarm messages, performance reports, and at the top of the Main menu. You can specify any name up to 15 characters long. Usually you specify a name that represents your site or the service you are connected to.

The device name specified here is also the name returned with the MIB II *sysName* object.

The default device name is “PORTLAND,OR.”

The device name is stored in the permanent nonvolatile configuration database.

## Using the command line

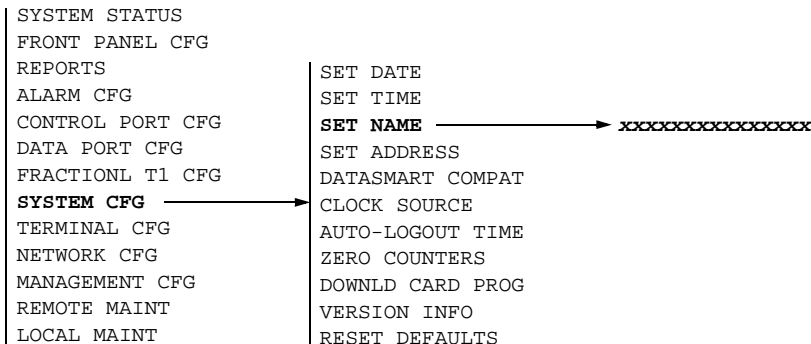
You change the device name by using the **SN** command. You must have super-user or configuration privileges. The command syntax is:

**SN:***id*

*id* Enter the device name. The name can be up to 15 characters long, including spaces, commas, or colons. A space, comma, or colon may not appear in the first position. Trailing spaces are truncated. DataSMART MAX automatically converts all alphabetic characters to uppercase.

## Using the front panel

A name entered via the front panel can be 15 characters long. To set the name from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display.
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until SET NAME appears in the display.
- 5 Push Select. The current device name appears in the display.
- 6 Push Next or Previous to select the character in the field you want to change. When the character field you want to change is underlined, push Select.
- 7 Push Next or Previous to change the character. When the character you want is displayed, push Select.

- 8 Repeat steps 6 and 7 until you have changed all the character fields you want.
- 9 Push Escape. SET NEW STRING? appears in the display. Push Select or push Escape to abort.

## Specifying an address

### TIP

The device address is not the same as the IP address. See “Setting the IP addresses and net-masks” on page 160 for instructions on setting the IP address.

When multiple DataSMART MAX units are configured in a daisy-chain, you must assign each a unique address. A daisy-chain allows you to log into multiple DataSMART MAX units through one control port — that way you do not need a separate terminal for each DataSMART MAX. The unique address makes it possible for you to specify which DataSMART MAX in the daisy chain you want to log into.

Typically you will connect the DataSMART MAX units into a daisy chain and then use the front panel to assign addresses to each one. However, it is possible to assign an address from the command line.

The default device address is 00:00:000. Do not change the address unless you are putting the DataSMART MAX in a daisy chain.

The device address is stored in the permanent nonvolatile configuration database.

### Using the command line

To set the device address, use the **SA** command. You must have super-user or configuration privileges. The syntax for the command is:

**SA:xx,yy,zzz**

The allowed values for the three address fields are:

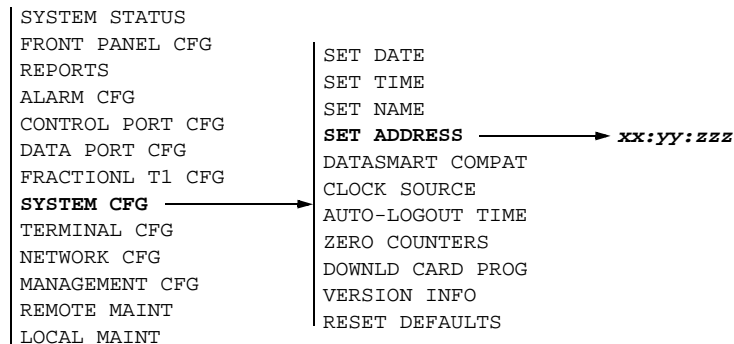
xx = 0 - 15

yy = 0 - 15

zzz = 0 - 255

### Using the front panel

To set the device address from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display.
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until SET ADDRESS appears in the display.

- 5 Push Select. The current address appears in the display.
- 6 Push Next or Previous to move between address fields. When the field you want to change is underlined, push Select.
- 7 Push Next or Previous to change the value in the field. When the value you want is displayed, push Select or push Escape to abort.
- 8 Repeat steps 6 and 7 until the address fields are correct.

### Logging in with an address

You do not need to log into a stand-alone device with an address of 00:00:000. Simply push the Enter key on your terminal, then enter your password (if passwords have been established).

To log into a device in a daisy chain, enter:

```
<Ctrl-D>xx:yy:zzz<Ctrl-E>
```

where *xx:yy:zzz* is the address of the device (the delimiting colons are required). This will bring up the Main menu of the device.

To log out of a device, enter:

```
<Ctrl-D>
```

### Enabling/disabling the front panel

To secure the front panel, you need to set a front-panel password, then enable or disable the front-panel controls as desired. For more information, see Chapter 2, “[Securing the front panel](#)”, on [page 33](#).

### Specifying DataSMART compatibility

Refer to “[Commands available via ARC](#)” on [page 198](#) for a discussion of how to enable and disable DataSMART compatibility with the **EDC** and **DDC** commands.

### Specifying the system clock

The DataSMART MAX uses one source clock to time all outputs. This includes outputs at the network interface, at the data ports, and at the terminal interface (if one exists).

For most applications, the DataSMART MAX is set to derive its source clock from the network receive signal (Loop Timing). This is the most common timing setup and should be used if your T1 service provider supplies timing. If your T1 service provider does not supply timing, you must select an alternate source as specified in Table 2.

Figure 4 illustrates some common timing applications. When setting up your T1 circuit timing, it is important to remember this general rule: **There must be one and only one timing source for the T1 circuit.**

The default is Loop Timing (i.e., the network receive signal).

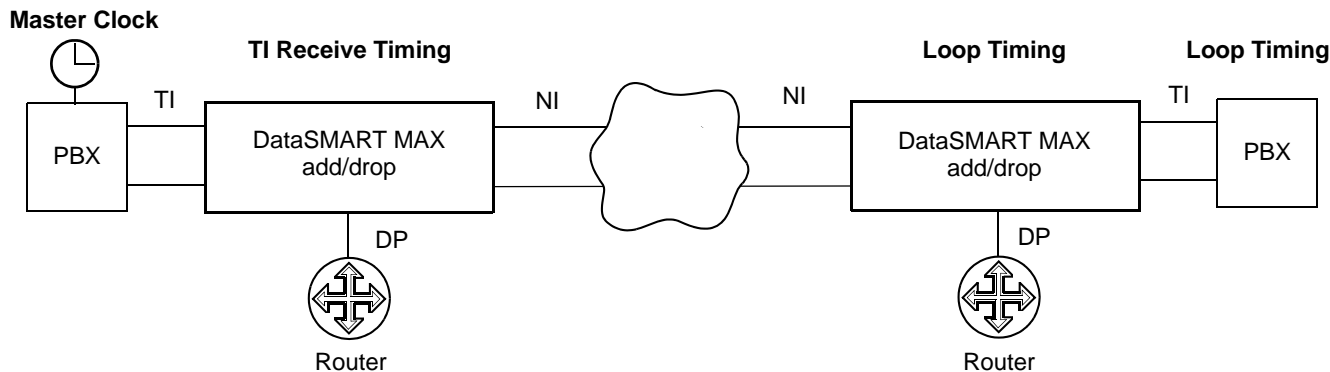
The system clock source is stored in the permanent nonvolatile configuration database.

**Table 2—Timing options**

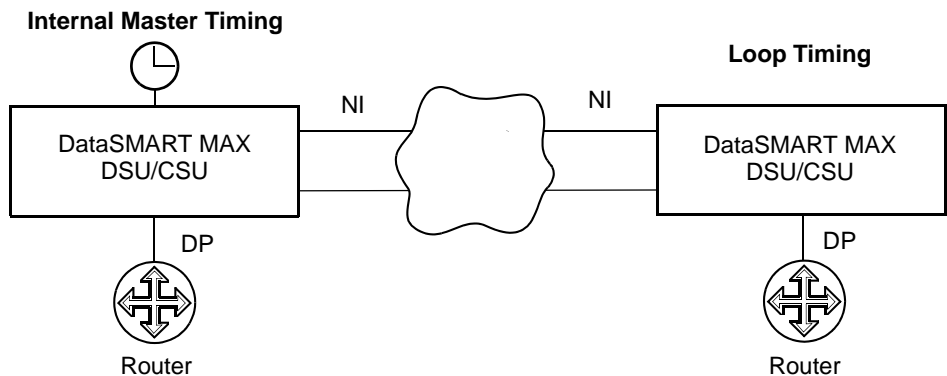
<b>Timing option</b>	<b>Description</b>
Loop Timing ( <b>L</b> )	<p>This option tells the DataSMART MAX to derive its system clock from the incoming signal at the network interface.</p> <p>Select this option if: 1) the T1 service provider is supplying a timing source, or 2) you are using the far-end device in a point-to-point connection as the master timing source.</p>
TI Receive Timing ( <b>T</b> )	<p>This option tells the DataSMART MAX to derive its system clock from the incoming signal at the terminal interface.</p> <p>Select this option if: 1) the T1 service provider is not supplying a timing source, and 2) you want to receive timing from a device beyond the terminal interface, such as a PBX.</p>
Internal Master Timing ( <b>I</b> )	<p>This option tells the DataSMART MAX to use its internal oscillator as the system clock. In this case, the DataSMART MAX becomes the master in a point-to-point connection. The far-end device should be set to Loop Timing.</p> <p>Select this option only if the T1 service provider is not supplying a timing source.</p>
External Master Timing ( <b>E</b> )	<p>This option tells the DataSMART MAX to derive its system clock from the signal supplied at the Auxiliary connector on the rear-panel.</p> <p>Select this option only if you must synchronize the DataSMART MAX to a locally generated clock signal. No other timing can be supplied to the device.</p>
Data Port Timing ( <b>D</b> )  (This is also known as Tail Circuit Timing)	<p>This option tells the DataSMART MAX to derive its system clock from the signal being received at the XCLK pin on the specified data port connector. Data ports that select tail circuit timing must use the tail circuit timing cable.</p> <p>The data port configuration must be set to the data rate received, and the clock supplied must meet the network accuracy standard of <math>\pm 32</math> ppm.</p> <p>Select this option only if the T1 service provider is not supplying a timing source and the timing source is the device connected to the specified data port.</p>

Figure 4—Common timing applications

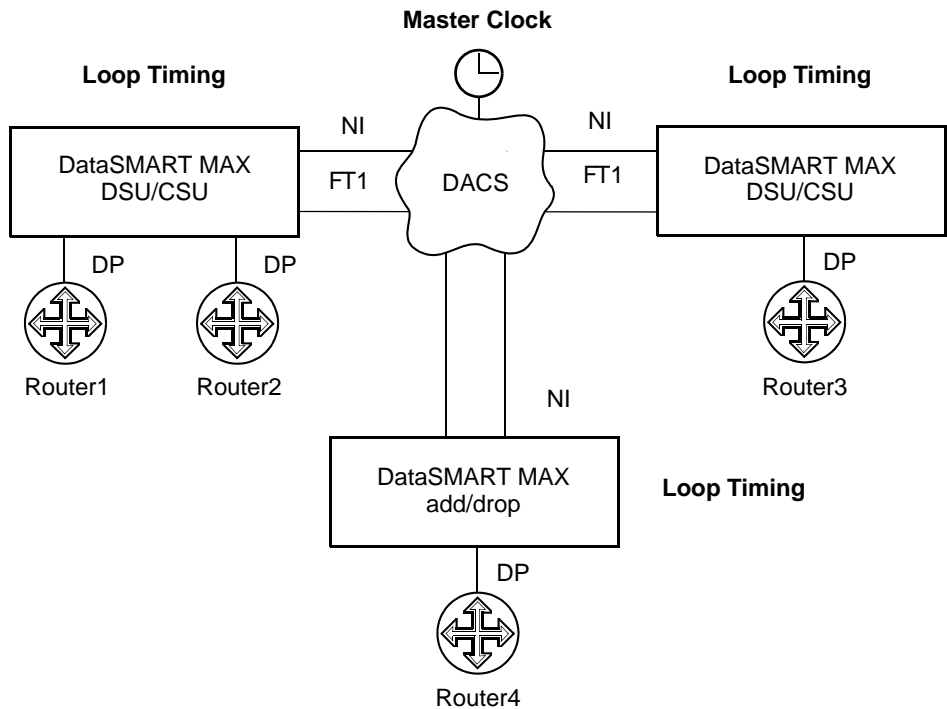
POINT-TO-POINT ADD/DROP APPLICATION: SPAN UNTIMED



POINT-TO-POINT DSU/CSU APPLICATION: SPAN UNTIMED



FRACTIONAL T1 DSU/CSU APPLICATION: SPAN TIMED BY CARRIER



## Secondary clock source

If the expected timing source is not present or is lost, DataSMART MAX defaults to Internal Master Timing. This occurs under the conditions specified in Table 3.

**Table 3—Conditions that cause a default to internal timing**

Timing option	Condition
Loop Timing	The DataSMART MAX defaults to internal timing if it cannot detect a clock in the incoming signal at the network interface, either because the signal is lost or because the signal is out of frame or AIS is detected.
TI Receive Timing	The DataSMART MAX defaults to internal timing if it cannot detect a clock in the incoming signal at the terminal interface, either because the signal is lost or because the signal is out of frame or AIS is detected.
External Master Timing	The DataSMART MAX defaults to internal timing if it cannot detect an external clock signal at the rear-panel Auxiliary connector.
Data Port Timing	The DataSMART MAX defaults to internal timing if it cannot detect an XCLK signal at the specified data port, either because a clock signal is not present or a DPLOS has occurred.

## Using the command line

You set the DataSMART MAX source clock by using the **CLK** command. You must have super-user or configuration privileges. The command syntax is:

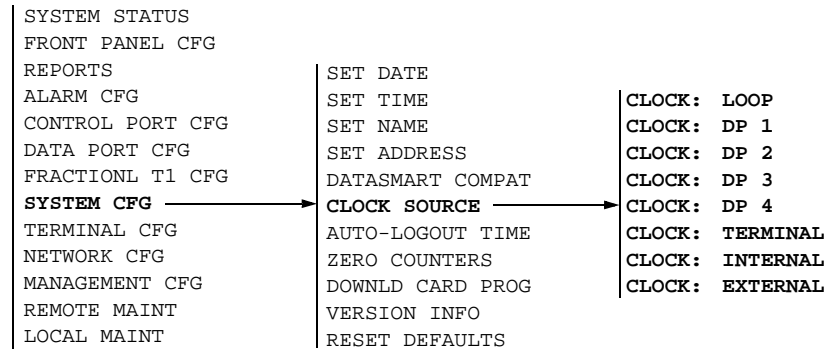
**CLK:***src*

The *src* value specifies the source clock as:

<b>L</b>	Loop Timing
<b>T</b>	TI Receive Timing
<b>I</b>	Internal Master Timing
<b>E</b>	External Master Timing
<b>1... 4</b>	Data Port Timing (also known as Tail Circuit Timing). You specify the data port number: 1 or 2 in a dual-port device; 1, 2, 3, or 4 in a quad-port device. The ports are numbered on the front panel.

## Using the front panel

To specify the clock source from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until CLOCK SOURCE appears in the display.
- 5 Push Select. The current clock setting appears in the display.
- 6 Push Next or Previous to cycle through the clock options. When the option you want appears in the display, push Select or push Escape to abort.

## Setting auto-logout for the control port

You can program DataSMART MAX to automatically log out a user who has been inactive for a specified period of time. This feature helps prevent situations where:

- A user with a high privilege level forgets to log out and leaves the DataSMART MAX open to other users.
- A user forgets to log out and blocks other users from logging in.
- A Telnet or ARC connection breaks down and hangs the connection.

You can specify an auto-logout of 0 (off), or from 1 to 60 minutes, inclusive. A setting of 0 disables the auto-logout timer for users who log in via a serial device connected to the control port. It does not disable the timer for users who log in via Telnet or ARC — you cannot disable auto-logout for these types of remote logins. When the timer is set to 0, DataSMART MAX defaults to a 15-minute auto-logout period for Telnet or ARC.

The default for auto-logout is 0 (off).

The auto-logout value is stored in the permanent nonvolatile configuration database.



### Using the command line

To specify an auto-logout period for the control port, use the **ALGOUT** command. When you set the timer to a value greater than 0, that value is used as the auto-logout period for the control port, and for Telnet and ARC logins.

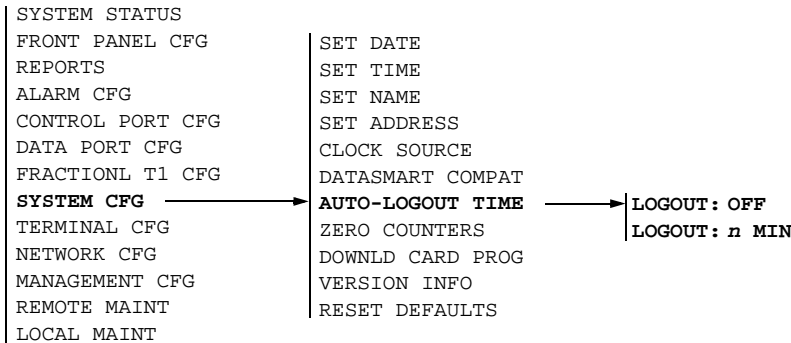
You must have super-user or configuration privileges to use the **ALGOUT** command. The command syntax is:

**ALGOUT:***n*

*n* Specify the auto-logout period in minutes, from 1 to 60, inclusive. 0 disables the timer (the auto-logout period for Telnet and ARC logins becomes 15 minutes).

### Using the front panel

To specify an auto-logout for the control port from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until AUTO-LOGOUT TIME appears in the display.
- 5 Push Select. The current timer setting appears in the display.
- 6 Push Next or Previous to cycle through the timer options: 1 - 60, or OFF. When the option you want appears in the display, push Select or push Escape to abort.

### Setting auto-logout for the front panel

The front-panel auto-logout feature prevents you from inadvertently leaving the front panel in an enabled state. See [“Securing the front panel” on page 33](#) for more information.

## Zeroing all counters

If you change the configuration parameters for the DataSMART MAX, you may want to clear the performance database. You do this by zeroing all counters. This clears the data from the following:

- User NI Short and Long Performance reports
- User TI Short and Long Performance reports
- Far-end PRM Short and Long Performance reports
- User NI Statistical Performance report
- User TI Statistical Performance report
- Error threshold counters

It does not clear the data from:

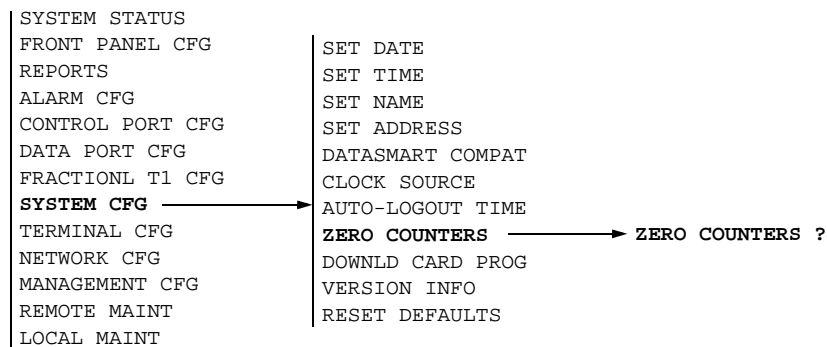
- Carrier NI Short and Long Performance reports
- Alarm History report

### Using the command line

To zero the counters, use the **ZALL** command. You must have super-user or configuration privileges.

### Using the front panel

To zero the counters from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display.
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until ZERO COUNTERS appears in the display.
- 5 Push Select. ZERO COUNTERS? appears in the display.
- 6 Push Select again to zero the counters, or push Escape to abort. If you push Select, the message PERF DATA CLEARD is displayed, indicating that the counters have been zeroed.

# Obtaining product version information

If you call Kentrox Technical Support, you should have the model and serial numbers for your DataSMART MAX available to give to your representative. You can obtain this information from the command line or the front panel.

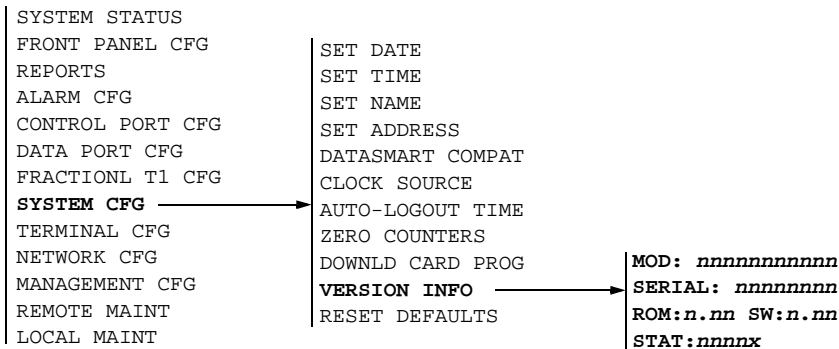
## Using the command line

Use the **WYV** command to obtain version information. You need super-user, configuration, or maintenance privileges. The DataSMART MAX displays the version information on the screen.

```
KENTROX      01-72775, SERIAL 00123456,  
STAT 0707E, ROM VER 1.31, S/W VER 1.31
```

## Using the front panel

To obtain version information from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display.
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until VERSION INFO appears in the display.
- 5 Push Select, then push Next or Previous to cycle through the version information.

# Resetting to default values

You can reset the DataSMART MAX to its default power-up state at any time. The DataSMART MAX will:

- Log out all users
- Restart its control program and execute self test
- Reset all configuration parameters to their default state, including bandwidth assignments
- Zero counters in the performance reports and clear the Alarm History report

Once self-test has been completed, you can log into the unit.



### CAUTION!

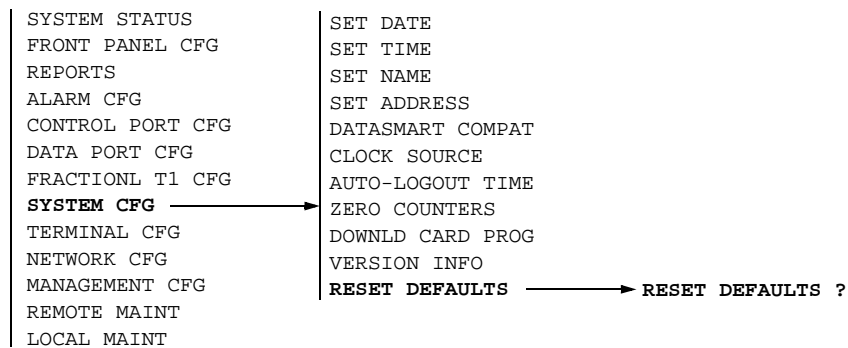
A reset to defaults causes a service disruption until the DataSMART MAX is reconfigured for service.

### Using the command line

To reset the DataSMART MAX to its default configuration, use the **RSD** command. You must have super-user or configuration privileges.

### Using the front panel

To reset defaults from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until SYSTEM CFG appears in the display.
- 3 Push Select. SET DATE appears in the display.
- 4 Push Next or Previous until RESET DEFAULTS appears in the display.
- 5 Push Select. RESET DEFAULTS? appears in the display. Push Select, or push Escape to abort.

---

## Configuring the control port

You need to set up the control port parameters if you are communicating with the DataSMART MAX via its DCE or DTE control port. This includes using a terminal, a modem, or a SLIP connection for Telnet or SNMP.

There are five steps to using a control port:

- 1 Make the physical cable connection between the port and the control device.
- 2 Establish the character protocol for the connection, including baud rate, parity, data bits, and stop bits.
- 3 Specify whether or not you want characters received at the control port to be echoed back to the control device.
- 4 Specify which control port you are using, either DCE or DTE.
- 5 Specify that your IP network interface is SLIP if you are using SLIP for Telnet or SNMP.



### NOTE

*When the unit is configured for SLIP, only IP packets are recognized on the control port. Therefore, you should set up your IP configuration as described in Chapter 7 before selecting SLIP.*

Step 1 is covered thoroughly in your *DataSMART MAX T1/FT1 Installation Guide*. This section does not repeat that information.

Steps 2, 3, and 4 are covered in this section.

Step 5 is covered in Chapter 7, under [“Selecting the IP network interface”](#) on [page 171](#).

## Command-line access

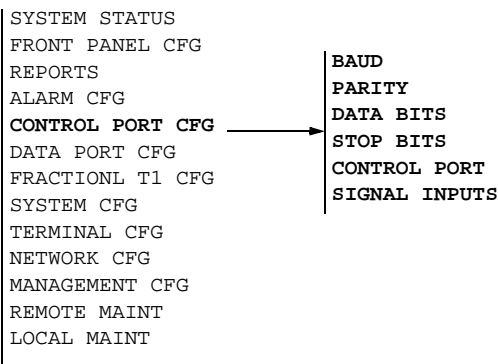
The commands for configuring control ports are listed below (enter **CC** to see this display).

```
CONTROL PORT CONFIGURATION MENU

EE / DE - Enable/Disable Character Echo
DCE/DTE - Select the Control Port
CCV      - View Control Port Configuration
```

## Front-panel access

The front-panel commands for configuring the control port are as follows.



## Viewing the current configuration

Before changing the control port parameters, you may want to look at the current settings. You can do this by executing the **CCV** command. This command displays the View Control Port Configuration screen, as shown below.

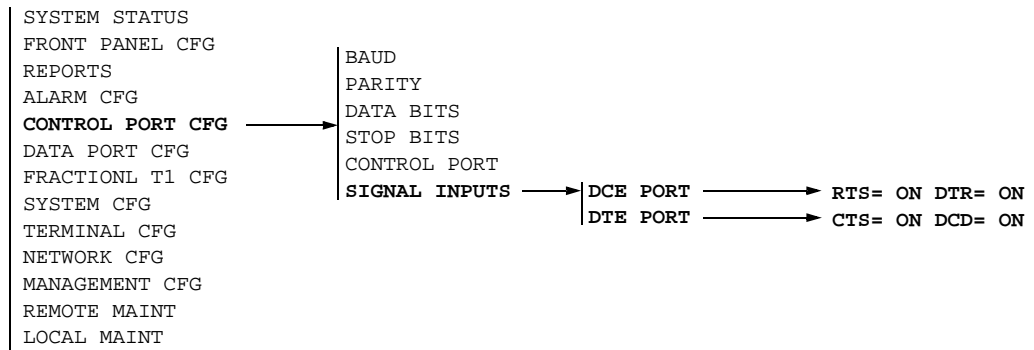
```
VIEW CONTROL PORT CONFIGURATION

Echo      Control Port    Daisy Chain    CP Setup
-----
ENABLED    DCE                    DISABLED        96,N,8,1

DCE Inputs  DTE Inputs
-----
RTS    DTR    CTS    DCD
---    ---    ---    ---
ON     ON     OFF    OFF
```

Field	Description
Echo	This field tells you if character echo is currently enabled or disabled.
Control Port	This field tells you the port at which DataSMART MAX will receive commands and output alarm messages.
Daisy Chain	This field tells you if daisy-chaining is enabled or disabled.
CP Setup	This field tells you the protocol settings of the control port: baud rate (in units of “hundreds”), parity, data-bits-per-character, and stop-bits-per-character.
DCE Inputs	These fields tell you the control port input signal state for RTS and DTR. Possible values for each include ON or OFF.
DTE Inputs	These fields tell you the control port input signal state for CTS and DCD. Possible values for each include ON or OFF.

## Using the front panel to view DCE or DTE inputs



### **TIP**

*Both input signals must be on before you can communicate through the selected control port.*

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until CONTROL PORT CFG appears in the display.
- 3 Push Select. BAUD appears in the display.
- 4 Push Next or Previous until SIGNAL INPUTS appears in the display.
- 5 Push Select. DCE PORT appears in the display.
- 6 Push Next or Previous if you want to change to the DTE port.
- 7 Push Select to view the current input states for the port.

# Configuring the physical connection

By default, the DataSMART MAX is set up with the following character protocol:

```
baud = 9600
parity = NONE
data bits-per-character = 8
stop bits-per-character = 1
```

If the control device you are using is set differently than the DataSMART MAX, you can change the settings on the control device, or you can change the settings in the DataSMART MAX.

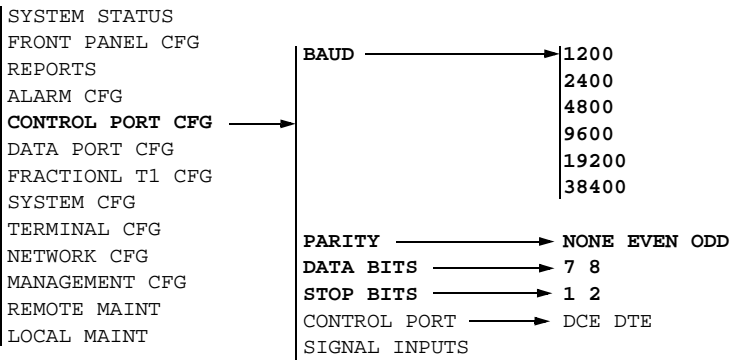
All settings apply to both control ports: DCE and DTE.

The settings are stored in the permanent nonvolatile configuration database.

You cannot change the protocol settings via the command line.

## Using the front panel

To change the protocol settings from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until CONTROL PORT CFG appears in the display
- 3 Push Select. BAUD appears in the display.
- 4 Push Select if you want to change the baud rate. The currently configured baud rate appears in the display.
- 5 Push Next or Previous until the desired baud rate appears in the display.
- 6 When the correct baud rate is displayed, push Select to choose that baud rate.
- 7 Repeat steps 4 through 6 for PARITY, DATA BITS, and STOP BITS. Push Next or Previous to to move between the displayed choices. When the choice you want is blinking, push Select.

Allowed parity settings are: NONE, EVEN, or ODD.

Allowed data-bits-per-second: 7 or 8.

Allowed stop-bits-per-second: 1 or 2.



## Enabling/disabling character echo

When character echo is enabled, all printable characters sent to the control port are echoed back to the control device (e.g., characters are echoed on the screen of the control device). If character echo is disabled, characters are not echoed back to the control device.

The default for character echo is “enabled”.

The state of character echo is stored in the permanent nonvolatile configuration database.

### Using the command line

You can use the **EE** and **DE** commands to enable or disable character echo. You must have super-user or configuration privileges.

<b>EE</b>	Enable character echo.
<b>DE</b>	Disable character echo.

You cannot enable or disable character echo from the front panel.

## Specifying the control port

When you specify either DCE or DTE, you are telling the DataSMART MAX which physical control port to use. The DataSMART MAX will expect to receive commands via that port and will output all alarm messages or SNMP traps to that port.

If you are communicating with the DataSMART MAX by modem, the modem will be connected to the DTE control port. In this case, use the commands described below to set the control port to DTE. In all other cases, the control device will be connected to the DCE port and you should leave the control port set to DCE.

If you are using a modem with daisy-chained DataSMART MAX units, you must program each device in the daisy chain to use the DTE control port.

The control port setting does not take effect until you have logged out, then logged back into the DataSMART MAX.

The default control port is DCE.

The control port setting is stored in the permanent nonvolatile configuration database.

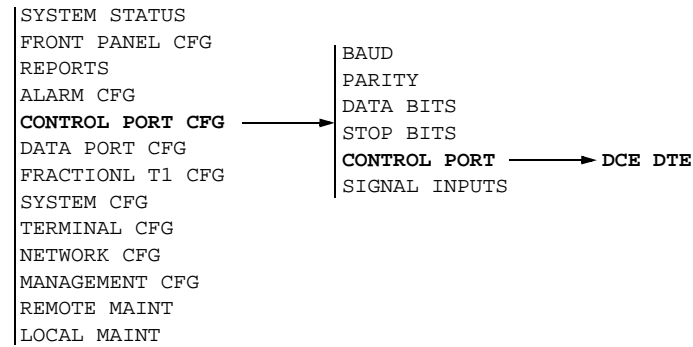
### Using the command line

To specify the control port, use the **DCE** or **DTE** command. You must have super-user or configuration privileges.

<b>DCE</b>	Use this if any device other than a modem is connected to the control port.
<b>DTE</b>	Use this if a modem is connected to the control port.

## Using the front panel

To specify the control port from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until CONTROL PORT CFG appears in the display.
- 3 Push Select. BAUD appears in the display.
- 4 Push Next or Previous until CONTROL PORT appears in the display.
- 5 Push Select. DCE DTE appears in the display. The current control port is blinking.
- 6 Push Next or Previous to change the current control port. When the desired value is blinking, push Select.

---

## Configuring alarms

As part of the overall system setup, you can specify the format and types of alarm messages output by the DataSMART MAX. You can:

- Enable or disable the generation of alarm messages.
- Specify the alarm message format as human-readable or as SNMP traps.
- Set the errored second (ES) and unavailable second (UAS) thresholds upon which EER alarms are generated.
- Specify the “sliding” time period for ES or UAS threshold evaluation.
- Specify whether or not an alarm should be generated on an incoming yellow condition.
- Specify the duration of the DataSMART MAX alarm deactivation period.

This section describes how to set up the configuration parameters for alarms. If you enable alarms, you may also need to specify which control port you are using, DCE or DTE, so that alarms are output correctly (see [“Specifying the control port” on page 57](#)). By default, the alarms are output to DCE.

If you are using an SNMP network management tool, you will also need to make sure your IP network interface is properly configured so that traps are sent to the right destination (see Chapter 7, [“Using network management”](#)).

### Command-line access

The commands for configuring alarms are listed below (enter **AC** to see this display).

```
ALARM CONFIGURATION MENU

EAM / DAM      - Enable/Disable Alarm Messages
EUM / ESM      - User/SNMP Alarm Message Format.

EYL / DYL      - Enable/Disable YELLOW Activating an Alarm
DACT:<n>       - Alarm Deactivation time in seconds, n = 1..15
EST:<n>        - Errored Second Threshold, n = 0 .. 900
UST:<n>        - Unavailable Second Threshold, n = 0 .. 900
ST15/ ST60     - Set Threshold Timing to 15 or 60 Minutes

ACV           - View Alarm Configuration
```

## Front-panel access

The front-panel commands for configuring alarms are as follows.

SYSTEM STATUS		ALARM MESSAGES
FRONT PANEL CFG		ALARM FORMAT
REPORTS		YEL ACTIVATE ALM
ALARM CFG	→	ES THRESHOLD
CONTROL PORT CFG		UAS THRESHOLD
DATA PORT CFG		THRESHOLD TIMING
FRACTIONL T1 CFG		ALARM DEACT TIME
SYSTEM CFG		
TERMINAL CFG		
NETWORK CFG		
MANAGEMENT CFG		
REMOTE MAINT		
LOCAL MAINT		

## Viewing the current configuration

Before changing the alarm configuration parameters, you may want to look at the current settings. You can do this by executing the **ACV** command. This command displays the Alarm Configuration screen, as shown below.

VIEW ALARM CONFIGURATION		
Message	Alarms Activated	Alarm Deactivation
	LOS+AIS+OOF	Seconds
-----	-----	-----
DISABLE	+YEL+EER	15
EST	UST	Threshold
		Timing
---	---	-----
13	10	15

Field	Description
Message	This field tells you if alarm messages are enabled or disabled. If alarms are enabled, the field tells you the message format, either USER (ASCII) or SNMP.
Alarms Activated	This field tells you what types of conditions will generate alarms. LOS, AIS, and OOF always generate alarms; you can enable or disable alarms for EER and incoming yellow.
Alarm Deactivation Seconds	This field tells you how many seconds the DataSMART MAX will continue in an alarm state once the alarm condition has been cleared.
EST, UST	These fields tell you the alarm thresholds for errored second (ES) and unavailable second (UAS), respectively. A zero (0) value means that EER alarms for ES or UAS have been disabled.
Threshold Timing	This field tells you the “sliding” time period that the DataSMART MAX is using for ES and UAS threshold evaluation. The period can be either 15 or 60 minutes.

# Enabling/disabling alarm messages

The DataSMART MAX outputs an alarm message to your control device when it enters an alarm state. This message identifies the alarm type, the time and date of the alarm occurrence, and the device name and address of the DataSMART MAX sending the message.

You can disable this alarm message output. For example, you may want to do this if you are using a “polling” program to monitor alarms on the devices in your network.

The default for alarm message output is “disabled”.

The state of the alarm message output is stored in the permanent nonvolatile configuration database.



## NOTE

*Disabling alarm messages does not affect the other alarm reporting mechanisms in the DataSMART MAX, including the Alarm History report, the System Status report, and LED illumination.*

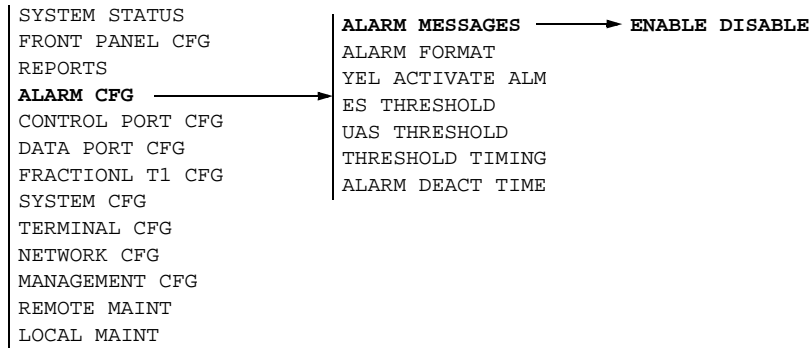
## Using the command line

To enable or disable alarm messages from the command line, use the **EAM** and **DAM** commands. You need super-user or configuration privileges.

<b>EAM</b>	Enable alarm messages.
<b>DAM</b>	Disable alarm messages.

## Using the front panel

To enable or disable alarm messages from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Select. ENABLE DISABLE appears in the display with the current selection blinking.
- 5 Push Next or Previous to change the selection. When the desired choice is blinking, push Select.

Formatting the alarm messages (ASCII or SNMP)

DataSMART MAX outputs alarm messages in one of two formats:

- ASCII, suitable for terminals and printers
- SNMP traps, suitable for SNMP network management systems

Specify the format appropriate for your application. If you are using an SNMP network management system, you will also need to configure your IP network interface and trap destinations properly (see Chapter 7, “Using network management”).

The default alarm format is ASCII.

The state of the alarm message format is stored in the permanent nonvolatile configuration database.

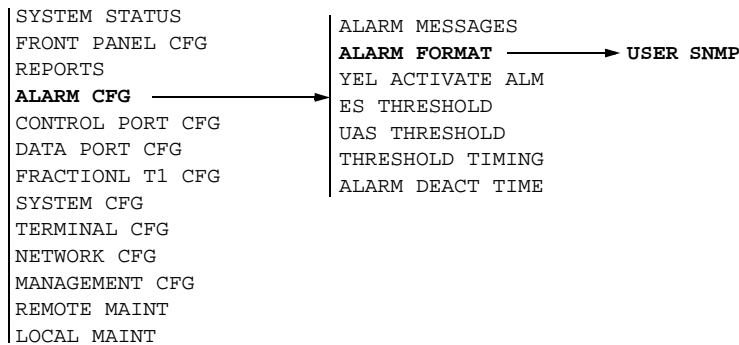
Using the command line

To specify the message format from the command line, use the **EUM** and **ESM** commands. You must have super-user or configuration privileges.

- EUM**                      Output alarm messages in the ASCII format.
- ESM**                      Output alarm messages as SNMP traps.

Using the front panel

To specify the format of alarm messages from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Next or Previous until ALARM FORMAT appears in the display.
- 5 Push Select. USER SNMP appears in the display with the current selection blinking.
- 6 Push Next or Previous to change the selection. When the desired choice is blinking, push Select.

Enabling/disabling  
alarms on incoming  
yellow

The DataSMART MAX generates an alarm message if it detects an incoming yellow alarm code at the network or terminal interface, and thus notifies you of a far-end problem. If you do not want this notification, you can deactivate this alarm message. You might also want to deactivate this alarm message if you are using SF framing and are receiving bit patterns that generate a false yellow indication.

The default is to generate an alarm message on incoming yellow (enabled).

The state of alarm message activation is stored in the permanent nonvolatile configuration database.

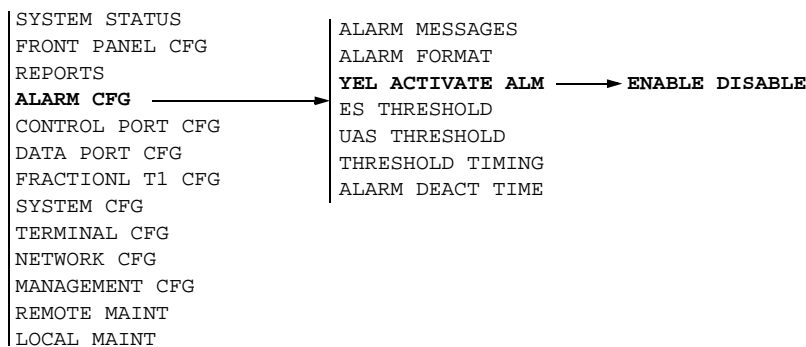
Using the command line

To enable or disable activation of an alarm on incoming yellow, use the **EYL** and **DYL** commands. You must have super-user or configuration privileges.

- EYL** Enable alarm activation on incoming yellow.
- DYL** Disable alarm activation on incoming yellow.

Using the front panel

To enable or disable alarm activation on an incoming yellow alarm, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Next or Previous until YEL ACTIVATE ALM appears in the display.
- 5 Push Select. ENABLE DISABLE appears in the display with the current selection blinking.
- 6 Push Next or Previous to change the selection. When the desired choice is blinking, push Select.

Setting the threshold for errored seconds (ES)

You can specify that the DataSMART MAX generate an EER alarm on excessive errored seconds (ESs). This allows you to monitor the line for errors and detect problems that are not described by signal loss or out-of-frame alarms.

You set up an EER alarm on excessive ESs by using the **EST** command to specify the error threshold. You can specify a threshold value of from 0 to 900, inclusive. A value of 0 disables EER alarm activation on errored seconds; a value of 900 means that an alarm will be generated if an ES occurs every second of a 15-minute time window (60 x 15).

You can set the time window to 15 minutes or 60 minutes by using the **ST15** or **ST60** command, respectively (see [page 66](#)). The window is a “sliding” window.

The default threshold is 13 errored seconds and the default window is 15 minutes (~10E<sup>-8</sup>).

The ES threshold is stored in the permanent nonvolatile configuration database.

Using the command line

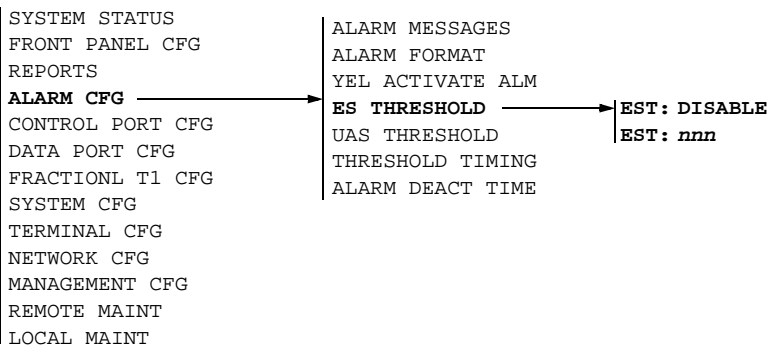
To set the ES threshold, use the **EST** command. You need super-user or configuration privileges. The command syntax is:

**EST:***n*

*n* Enter the number of ESs which must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables EER alarm activation on an ES condition.

Using the front panel

To set the ES threshold from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Next or Previous until the ES THRESHOLD appears in the display.
- 5 Push Select. The current threshold value appears in the display: 1 ... 900, or DISABLE (off).
- 6 Push Next or Previous to change to the desired value, then push Select.



# Setting the threshold for unavailable seconds (UAS)

If your line is experiencing chronically high error rates, you may elect to disable the errored second (ES) threshold and just use the unavailable second (UAS) threshold for generating EER alarms. This decreases the alarm sensitivity significantly, since a UAS occurs at the onset of ten consecutive severely errored seconds (SESSs).

You use the **UST** command to specify the threshold used for generating an EER alarm on UASs. You can specify a threshold value of from 0 to 900, inclusive. A value of 0 disables EER alarm activation on unavailable seconds; a value of 900 means that an EER alarm will be generated if an unavailable second occurs every second of a 15-minute time window (60 x 15).

You can set the time window to 15 minutes or 60 minutes by using the **ST15** or **ST60** command, respectively (see [page 66](#)). The window is a “sliding” window.

The default threshold is 10 unavailable seconds and the default time window is 15 minutes.

The UAS threshold is stored in the permanent nonvolatile configuration database.

## Using the command line

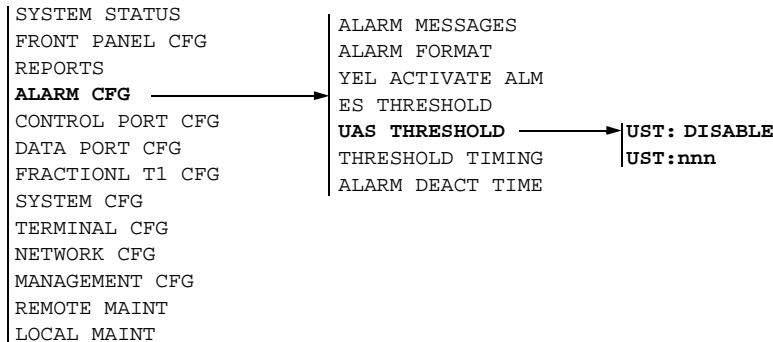
To set the UAS threshold, use the **UST** command. You need super-user or configuration privileges. The syntax for the command is:

**UST:***n*

*n* Enter the number of UASs which must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables alarm activation on a UAS condition.

## Using the front panel

To set the UAS threshold from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Next or Previous until UAS THRESHOLD appears in the display.
- 5 Push Select. The current threshold setting appears in the display.
- 6 Push Next or Previous to change to the desired value, then push Select.

## Specifying the threshold evaluation window

You can specify a 15-minute or a 60-minute “sliding” time window for error threshold evaluation. If the specified error threshold is exceeded during this sliding window, the DataSMART MAX generates an EER alarm. Use the 15-minute window for increased error sensitivity; use the 60-minute window for a longer term view of line quality.

The following table relates evenly distributed bit error rates and the number of ESs that will occur in 15- and 60-minute time periods.

Error rate	ESs in 15 minutes	ESs in 60 minutes
$1 \times 10^{-6}$	900	—
$1 \times 10^{-7}$	135	540
$1 \times 10^{-8}$	13	54
$1 \times 10^{-9}$	1	5

The default window for threshold evaluation is 15 minutes.

The window value is stored in the permanent nonvolatile configuration database.

### Using the command line

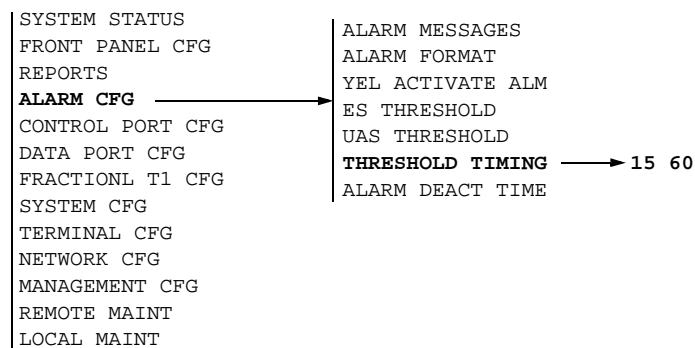
To specify the sliding window for threshold evaluation, use the **ST15** and **ST60** commands. You must have super-user or configuration privileges.

**ST15** Set the sliding window to 15 minutes.

**ST60** Set the sliding window 60 minutes.

### Using the front panel

To set the sliding window from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Next or Previous until THRESHOLD TIMING appears in the display.
- 5 Push Select. 15 60 appears in the display. The current value is blinking.
- 6 Push Next or Previous to change the value, then push Select.

# Setting the alarm deactivation time

You can program the DataSMART MAX to remain in an alarm state for up to 15 seconds after an alarm condition has cleared. This deactivation period applies to the following alarms:

- NI LOS and TI LOS
- NI AIS and TI AIS
- NI OOF and TI OOF
- NI YEL and TI YEL
- NI EER and TI EER

It does not apply to:

- ECF

The default alarm deactivation time is 15 seconds.

The alarm deactivation time is stored in the permanent nonvolatile configuration database.

## Using the command line

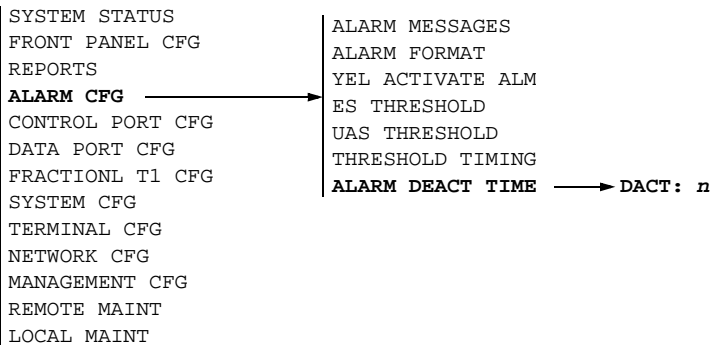
To set the alarm deactivation time, use the **DACT** command. You must have super-user or configuration privileges. The command syntax is:

**DACT:***n*

*n* Set the deactivation time from 1 to 15 seconds.

## Using the front panel

To set the alarm deactivation time from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until ALARM CFG appears in the display.
- 3 Push Select. ALARM MESSAGES appears in the display.
- 4 Push Next or Previous until ALARM DEACT TIME appears in the display.
- 5 Push Select. The current alarm deactivation period appears in the display: 1 ... 15 seconds.
- 6 Push Next or Previous to change the value, then push Select.



# 4

## *Configuring interfaces*

---

This chapter covers the following topics:

- Configuring the network interface
- Configuring the terminal interface
- Configuring data ports
- Assigning channels

---

# Configuring the network interface

The DataSMART MAX network interface should be configured to be compatible with the T1 signal received from the service provider. It is particularly important that the framing and line coding match those of the received signal. The other parameters are less critical, and the defaults supplied by the DataSMART MAX work for most applications.

## Command-line access

The commands for configuring the network interface parameters are listed below (enter NC to see this display).

```
NI CONFIGURATION MENU

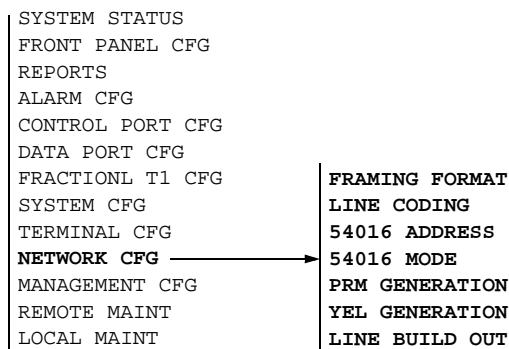
NSF/NESF/NERC  - NI SF/ESF/Ericsson Framing Format
NAMI / NB8     - NI AMI/B8ZS Line Coding
EPRM / DPRM    - Enable/Disable T1.403 PRM Generation out NI
EYEL / DYEL:    - Enable/Disable YELLOW Activation out NI
ADR54:<Trgt>    - 54016 Address = C(CSU), D(DSU), or B(Both)
E54 / D54      - Enable/Disable 54016 Mode

Line Build Out
NL0            - 0.0 dB
NL1            - 7.5 dB
NL2            - 15.0 dB

NCV            - View NI Configuration
```

## Front-panel access

The front-panel commands for configuring the network interface are as follows.



## Viewing the current NI configuration

You must set up the network interface parameters to match the requirements of your service provider. The DataSMART MAX framing format and line coding must match the framing format and line coding of your T1 line. Further, the DataSMART MAX line build out should always be left at 0.0 dB unless another value is specifically requested. Increased attenuation can interfere with the T1 service.

You can use the View Network Configuration display to see the current network interface settings. Enter **NCV** at the command-line prompt.

```
VIEW NETWORK CONFIGURATION

Framing Line Code Line Build Out PRM Generation
-----
SF      AMI      0.0 dB      DISABLED

YEL Generation 54016 Address 54016 Mode
-----
DISABLED      EITHER      ENABLED
```

Field	Description
Framing	This displays the current network framing: SF (super frame), ESF (extended super frame), or ERICS (Ericsson-modified super frame).
Line code	This displays the current line coding: AMI or B8ZS.
Line build out	This displays the state of line build out at the network interface. Possible values are 0.0 dB, 7.5 dB, or 15.0 dB.
PRM generation	This displays the state of ANSI T1.403 Performance Report Message (PRM) generation: ENABLED or DISABLED.
YEL generation	This displays the state of yellow alarm generation at the network interface: ENABLED or DISABLED.
54016 address	This displays the currently selected 54016 address filter: DSU, CSU, or CSU/DSU.
54016 mode	This displays the state of 54016 transmission: ENABLED or DISABLED.

## Specifying NI framing format

You must set the DataSMART MAX network interface to recognize and transmit data in the same framing format used by the incoming T1 line. Three format choices are available: super frame (SF), extended super frame (ESF), or Ericsson-modified super frame.

Note that if the incoming T1 line is in SF format, you may want to disable the DataSMART MAX from generating alarms upon detection of incoming yellow at the network interface. Sometimes data patterns in SF format generate false yellow. See [“Enabling/disabling alarms on incoming yellow” on page 63](#).

The default framing format is super frame (SF).

The framing format is stored in the permanent nonvolatile configuration database.

Using the command line

Use the following commands to specify framing format. You must have super-user or configuration privileges.

<b>NSF</b>	Super frame
<b>NESF</b>	Extended super frame
<b>NERC</b>	Ericsson-modified super frame

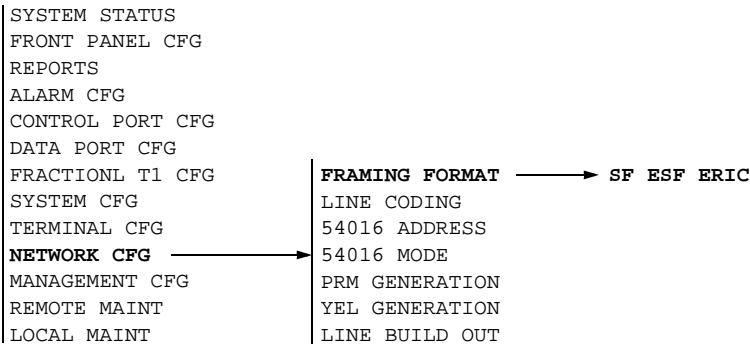


NOTE

*Framing format “NERC” is the framing format used by some L. M. Ericsson switches in the cellular service.*

Using the front panel

To specify framing format from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Select. SF ESF ERIC appears in the display. The currently selected format is blinking.
- 5 Push Next or Previous until the format you want is blinking, then push Select.



# Specifying NI line coding

You must set the DataSMART MAX network interface to the line coding specified by your service provider. Two selections are available: AMI (alternate mark inversion) or B8ZS (binary 8 zeroes substitution).

The default line coding is AMI.

The line coding is stored in the permanent nonvolatile configuration database.

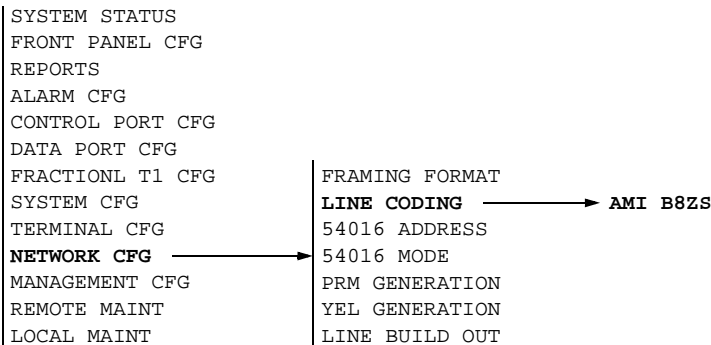
## Using the command line

Use the following commands to specify line coding. You must have super-user or configuration privileges.

<b>NAMI</b>	AMI line coding
<b>NB8</b>	B8ZS line coding

## Using the front panel

To specify line coding from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until LINE CODING appears in the display.
- 5 Push Select. AMI B8ZS appears in the display. The currently selected value is blinking.
- 6 Push Next or Previous until the line coding you want is blinking, then push Select.

Enabling/disabling  
T1.403 loopback and  
PRM generation

You can enable or disable the DataSMART MAX from sending and receiving ANSI T1.403 performance report messages (PRMs). When T1.403 mode is enabled, the DataSMART MAX does the following:

- Sends PRMs out the network interface to the far-end device
- Receives PRMs from the far-end device (used to collect data for far-end reports)
- Sets and resets remote loopbacks using T1.403-standard codes

When T1.403 mode is enabled, the DataSMART MAX defaults to T1.403 standards for setting and resetting loopbacks, even if 54016 mode is enabled.

The default state is T1.403 mode disabled.

The T1.403 mode is stored in the permanent nonvolatile configuration database.

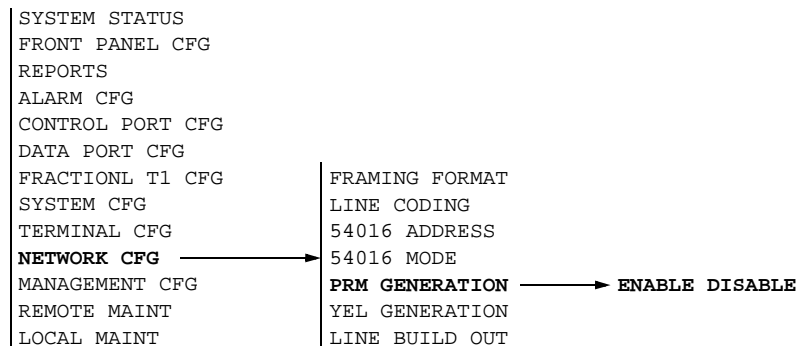
Using the command line

Use the following commands to enable or disable T1.403 mode. You must have super-user or configuration privileges.

- EPRM** Enable sending and receiving ANSI T1.403 PRMs and loopback set and reset codes.
- DPRM** Disable sending PRM messages to the network and disable all other activities defined by the standard.

Using the front panel

To enable or disable T1.403 mode from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until PRM GENERATION appears in the display.
- 5 Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
- 6 Push Next or Previous until the setting you want is blinking, then push Select.

# Enabling/disabling yellow alarm output

If enabled, the DataSMART MAX generates and transmits the yellow alarm code toward the network any time an alarm condition is detected on the network interface. The yellow alarm is transmitted two to three seconds after alarm conditions AIS, OOF or LOS arise.

If disabled, the DataSMART MAX will not generate a yellow alarm code. You may want to disable the alarm output if the DataSMART MAX is not the terminating device in your T1 network. If yellow is inserted in bit 2 (SF mode) and all channels are assigned to the TI, yellow will be passed through.

The default for alarm generation on incoming yellow is disabled.

The state of yellow alarm activation is stored in the nonvolatile configuration database.

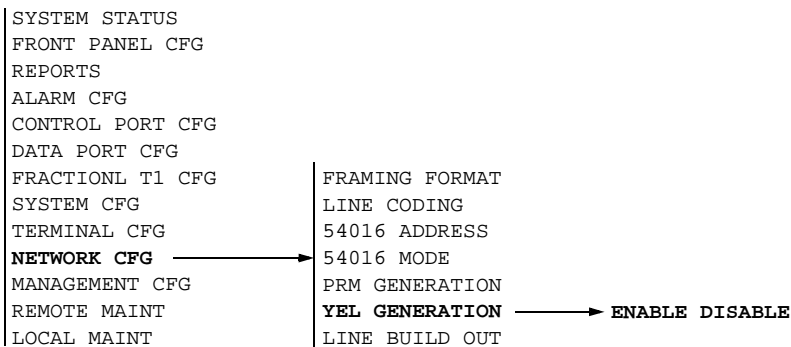
## Using the command line

Use the following commands to enable or disable yellow alarm generation. You must have super-user or configuration privileges.

- EYEL** Enable generation of yellow alarm.
- DYEL** Disable generation of yellow alarm.

## Using the front panel

To enable or disable yellow alarm generation from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until YEL GENERATION appears in the display.
- 5 Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
- 6 Push Next or Previous until the setting you want is blinking, then push Select.

# Selecting the 54016 address

If 54016 mode is enabled, you can specify whether the DataSMART MAX responds to 54016 requests addressed to a DSU, a CSU, or both. (See page 77 for procedures on enabling 54016 mode.)

If the DataSMART MAX is the only unit terminating the T1 network, you would normally set it to respond to both DSU and CSU requests. If you are using the DataSMART MAX in an add/drop application and have another 54016-compatible terminating device connected to the DataSMART MAX terminal interface, you may want to set the DataSMART MAX to respond to CSU requests only. It will then pass the DSU requests through to the other device.

The default is for the DataSMART MAX to respond to both CSU and DSU requests.

The setting is stored in the permanent nonvolatile configuration database.

## Using the command line

Use the following command to specify the 54016 address mode. You must have super-user or configuration privileges. The command syntax is:

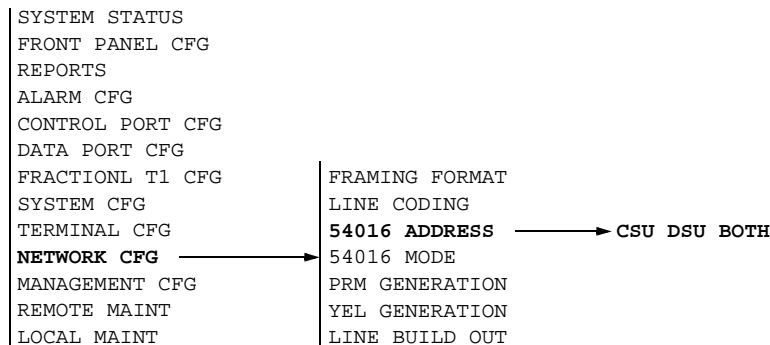
**ADDR54:***Trgt*

where *Trgt* is:

- D** DSU
- C** CSU
- B** both DSU and CSU

## Using the front panel

To specify the 54016 address mode from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until 54016 ADDRESS appears in the display.
- 5 Push Select. CSU DSU BOTH appears in the display. The currently configured value is blinking.
- 6 Push Next or Previous until the setting you want is blinking, then push Select.

# Enabling/disabling 54016 mode

You can enable and disable the DataSMART MAX from responding to requests that comply with the message format of AT&T TR54016, Issue 2. When enabled for 54016, the DataSMART MAX can do the following:

- Respond to 54016 requests
- Set and reset remote loopbacks using 54016 requests (if T1.403 is disabled see [“Enabling/disabling T1.403 loopback and PRM generation” on page 74](#)).

54016 requests are received and sent via the ESF facility data link. This means that the network interface must be set to ESF format in order for 54016 requests to work.

The default is 54016 mode disabled.

The 54016 mode is stored in the permanent nonvolatile configuration database.

## Using the command line

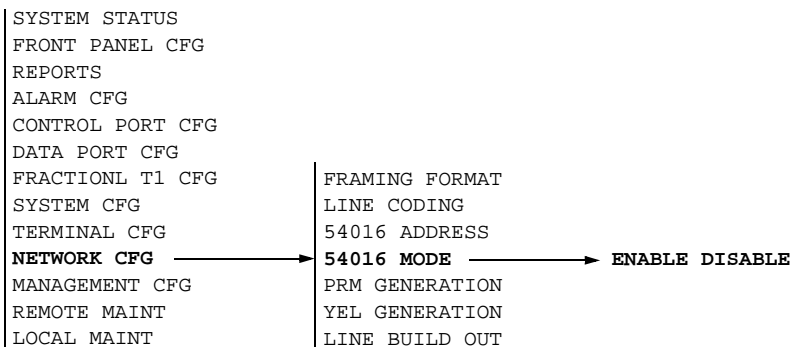
Use these commands to enable or disable 54016 mode. You must have super-user or configuration privileges.

**E54** Enable 54016 mode.

**D54** Disable 54016 mode.

## Using the front panel

To enable or disable 54016 mode from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until 54016 MODE appears in the display.
- 5 Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
- 6 Push Next or Previous until the setting you want is blinking, then push Select.

Specifying transmit  
line build out  
attenuation

As requested by your service provider, set the DataSMART MAX to attenuate the T1 signal before outputting it at the network interface. Three line attenuation settings are available: 0.0 dB (no attenuation), 7.5 dB, or 15 dB. Under normal conditions, leave the attenuation setting to 0.0 dB.

The default line attenuation is 0.0 dB.

The line attenuation is stored in the permanent nonvolatile configuration database.

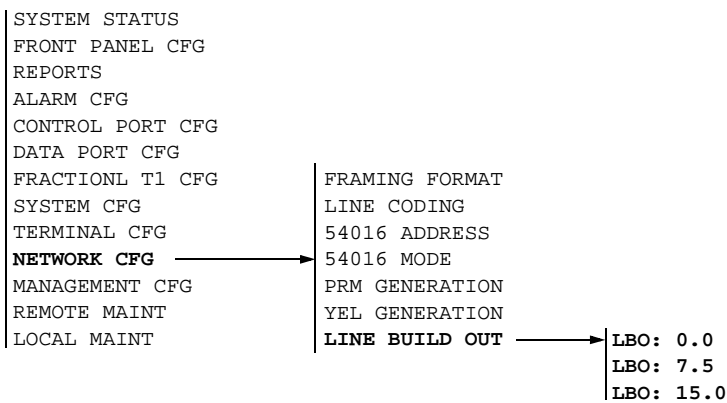
Using the command line

Use the following commands to specify line attenuation. You must have super-user or configuration privileges.

- NL0 0.0 dB line attenuation
- NL1 7.5 dB line attenuation
- NL2 15.0 dB line attenuation

Using the front panel

To specify line attenuation from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until NETWORK CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until LINE BUILD OUT appears in the display.
- 5 Push Select. The current LBO setting appears in the display.
- 6 Push Next or Previous to change the LBO setting to the one you want, then push Select.

---

# Configuring the terminal interface

You must configure the terminal interface of the Data SMART MAX to make it compatible with the terminal equipment connected to it.

## Command-line access

The commands for configuring the terminal interface parameters are listed below (enter TC to see this display).

```

TI CONFIGURATION MENU

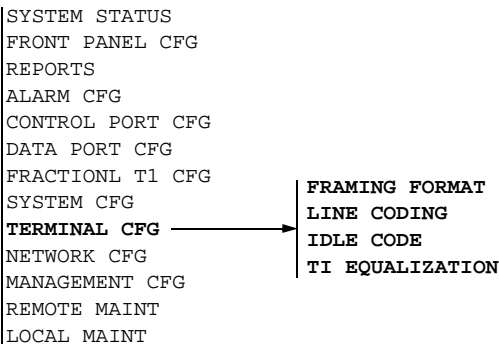
TSF/TESF/TERC - TI SF/ESF/Ericsson Framing Format
TAMI/TB8      - TI AMI/B8ZS TI Line Coding
TIDL:<c>       - Idle Code, c = 00-FF Hex

                TI Equalization
TE0            - 0 - 133 ft
TE1            - 133 - 266 ft
TE2            - 266 - 399 ft
TE3            - 399 - 533 ft
TE4            - 533 - 655 ft

TCV            - View TI Configuration
```

## Front-panel access

The front-panel commands for configuring the terminal interface are as follows.



## Viewing the current TI configuration

Before changing any terminal interface parameters, you may want to look at the current settings. To do this, enter **TCV** at the command-line prompt. This produces a display similar to the one below.

```
VIEW TERMINAL CONFIGURATION

Framing   Line   Equalization   Idle
Format    Code                Code
-----
ESF       B8ZS   133..266 ft   88 Hex
```

Field	Description
Framing format	This displays the current framing format applied to the terminal interface: SF (super frame), ESF (extended super frame), or ERICS (Ericsson-modified super frame).
Line code	This displays the current line coding applied to the terminal interface: AMI or B8ZS.
Equalization	This displays the state of signal equalization at the terminal interface: 0..133ft, 133..266ft, 266..399ft, 399..533ft, or 533..655ft.
Idle code	This displays the currently selected idle code. The range is 00 to FF hex.

## Specifying TI framing format

You must set the DataSMART MAX terminal interface to recognize and transmit data in the same framing format used by the terminating customer premises equipment, usually a T1 channel bank or digital PBX. Three format choices are available: super frame (SF), extended super frame (ESF), and Ericsson-modified super frame.

The default framing format is super frame.

The framing format is stored in the permanent nonvolatile configuration database.

### Using the command line

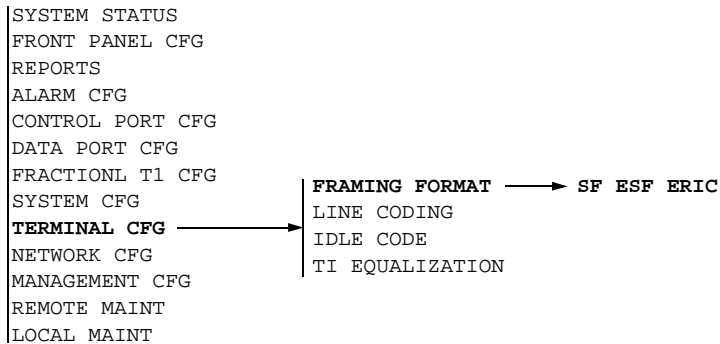
Use the following commands to set the framing format applied at the terminal interface.

<b>TSF</b>	Super frame
<b>TESF</b>	Extended super frame
<b>TERC</b>	Ericsson-modified super frame



### Using the front panel

To specify framing format from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until TERMINAL CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Select. SF ESF ERIC appears in the display. The currently configured value is blinking.
- 5 Push Next or Previous until the setting you want is blinking, then push Select.

### Specifying TI line coding

You must set the DataSMART MAX terminal interface to the same line coding used by the customer premises equipment. Two selections are available: AMI (alternate mark inversion) or B8ZS (binary 8 zeroes substitution).

The default line coding is AMI.

The line coding is stored in the permanent nonvolatile configuration database.

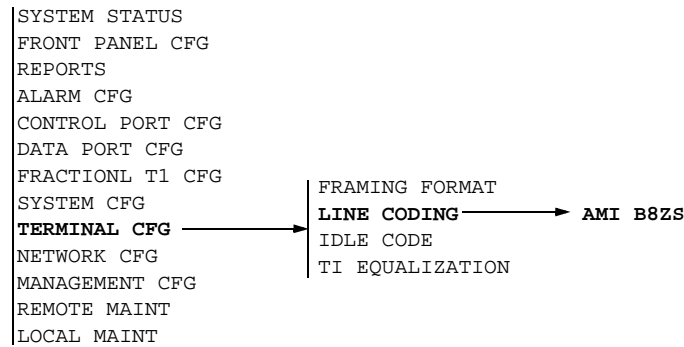
### Using the command line

Use the following commands to specify line coding. You must have super-user or configuration privileges.

<b>TAMI</b>	AMI line coding
<b>TB8</b>	B8ZS line coding

## Using the front panel

To specify line coding from the the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until TERMINAL CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until LINE CODING appears in the display.
- 5 Push Select. AMI B8ZS appears in the display. The currently configured value is blinking.
- 6 Push Next or Previous until the setting you want is blinking, then push Select.

## Specifying TI idle code

You can specify the eight-bit idle code that is put into the unused DS0 channels of the terminal interface. The code may have any hex value between 0x00 and 0xFF. This code is put into all DS0 channels assigned to the terminal interface during any out-of-frame condition at the interface. The idle code is also output at the terminal interface during network alarms.

The default idle code is 0x7F.

The idle code value is stored in the permanent nonvolatile configuration database.

## Using the command line

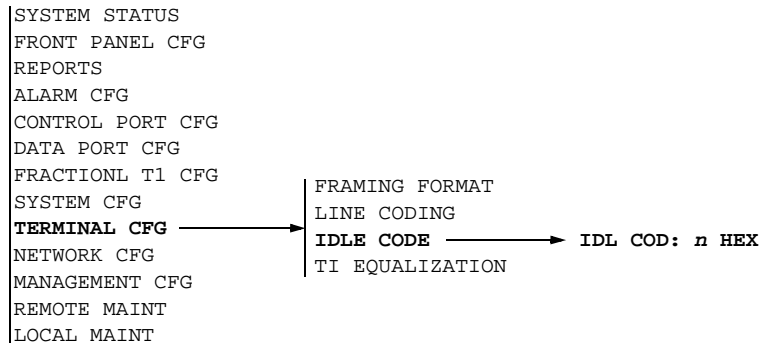
Use the **TIDL** command to specify the eight-bit idle code. You must have super-user or configuration privileges. The command syntax is:

**TIDL:***c*

*c* Enter a hex number with a value between 00 and FF.

## Using the front panel

To specify the idle code from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until TERMINAL CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until IDLE CODE appears in the display.
- 5 Push Select. The current idle code value appears in the display.
- 6 Push Next or Previous until the value you want appears in the display, then push Select.

## Specifying TI signal equalization

If the cable between the DataSMART MAX and the customer premises equipment is longer than 133 feet, you may need to boost the signal level being output from the terminal interface. Using the **TE***n* commands, you can specify that the terminal interface outputs a DSX-level signal equalized for cable lengths up to 655 feet.

The default equalization setting is 0.

The equalization setting is stored in the permanent nonvolatile configuration database.

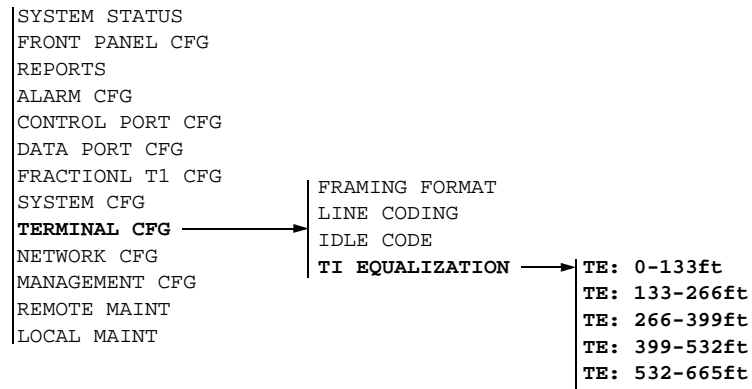
### Using the command line

Use the following commands to equalize the T1 signal at the terminal interface. You must have super-user or configuration privileges.

<b>TE0</b>	0 - 133 feet
<b>TE1</b>	133 - 266 feet
<b>TE2</b>	266 - 399 feet
<b>TE3</b>	399 - 533 feet
<b>TE4</b>	533 - 655 feet

## Using the front panel

To specify the signal equalization from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until TERMINAL CFG appears in the display.
- 3 Push Select. FRAMING FORMAT appears in the display.
- 4 Push Next or Previous until TI EQUALIZATION appears in the display.
- 5 Push Select. The current TI equalization configuration appears in the display.
- 6 Push Next or Previous until you see the equalization you want, then push Select.

---

# Configuring data ports

You must configure each data port to match the configuration of the data terminal equipment (DTE) to which it is attached.

Most applications can use the default values. “Tail” circuits, long DTE cables at high data rates, and perhaps other situations identified by your technical support representative may require changing the settings from their default values.

## Command-line access

The commands for configuring the data ports are listed below (enter **DC** to see this display).

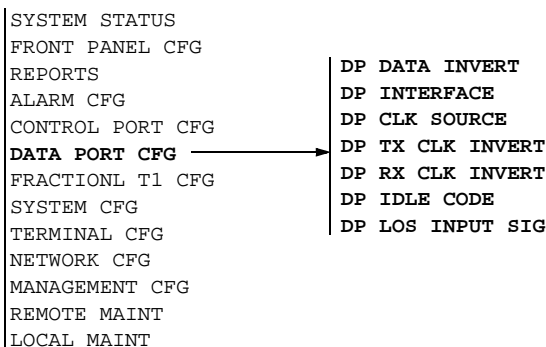
```
DATA PORT CONFIGURATION MENU

EDI<n> / DDI<n> - Enable/Disable Data Inversion at Data Port, n=1..4
INTF<n>:<intf> - Interface at Data Port, n=1..4
                  intf = V (V.35), E (EIA-530)
SCLK<n>:<clk> - Source Clock at Data Port, n=1..4
                  clk = I (Internal), E (External)
TCLK<n>:<cmd> - Transmit Clock Inversion at Data Port, n=1..4
                  cmd = E (Enable), D (Disable)
RCLK<n>:<cmd> - Receive Clock Inversion at Data Port, n=1..4
                  cmd = E (Enable), D (Disable)
IDL<n>:<char> - Idle Character at Data Port, n=1..4
                  char = 7E (0x7E), 7F (0x7F), FF (0xFF)
DPLOS<n>:<los> - LOS Input Signal at Data Port, n=1..4
                  los = R (RTS), D (DTR), B (Both), N (No Processing)

DCV - View Data Port Configuration
```

## Front-panel access

The front-panel commands for configuring the data ports are as follows.



## Viewing the current data port configuration

Before changing any data port parameters, you may want to look at the current settings. To do this, enter **DCV** at the command-line prompt. This produces a display similar to the one shown below.

```
VIEW DATA PORT CONFIGURATION

      Port 1      Port 2      Port 3      Port 4
      -----      -----      -----      -----
Data Inversion  DISABLED  DISABLED  DISABLED  DISABLED
Interface       V.35      V.35      V.35      V.35
Source Clock    INTERNAL  INTERNAL  INTERNAL  INTERNAL
Tx Clock Invert DISABLED  DISABLED  DISABLED  DISABLED
Rx Clock Invert DISABLED  DISABLED  DISABLED  DISABLED
Idle Character  0xFF     0xFF     0xFF     0xFF
LOS Input       RTS      RTS      RTS      RTS
```

Field	Description
<i>The columns identify the data ports to which the configuration applies.</i>	
Data Inversion	This tells you whether or not data inversion is enabled at the data port. If inversion is enabled, the data is inverted in both directions (i.e., the data from the DTE is inverted before being transmitted to the network, and vice versa).
Interface	This tells you the electrical interface specified for the data port: either V.35 or EIA-530.
Source Clock	This tells you which clock signal is being used to clock in transmit data at the data port: INTERNAL or EXTERNAL.
Tx Clock Invert	This tells you whether or not transmit clock inversion is enabled at the data port. If inversion is enabled, transmit data is sampled on the rising edge of the clock signal. If inversion is disabled, transmit data is sampled on the falling edge of the clock signal.
Rx Clock Invert	This tells you whether or not receive clock inversion is enabled. If inversion is enabled, receive data is changed on the falling edge of the clock signal. If inversion is disabled, receive data is changed on the rising edge of the clock signal.
Idle Character	This tells you the specified idle character for each data port: 0x7E, 0x7F, or 0xFF.
LOS Input	This tells you which signals are currently being used to determine an LOS condition at the data port: RTS, DTR, BOTH, or NONE.

Enabling/disabling data inversion

These commands invert data on selected data ports. When you enable data inversion, all data received from the DTE is inverted: zeroes are changed to ones and ones are changed to zeroes before being transmitted to the network. Data received from the network is also inverted before being transmitted to the DTE. When data is inverted locally, it must also be inverted at the far-end unit.

Data inversion is seldom necessary. It is sometimes used to resolve “ones density” problems caused by a high density of zeroes in the bit stream of the incoming or outgoing data.

The default state is data inversion disabled.

The data inversion state is stored in the permanent nonvolatile configuration database.

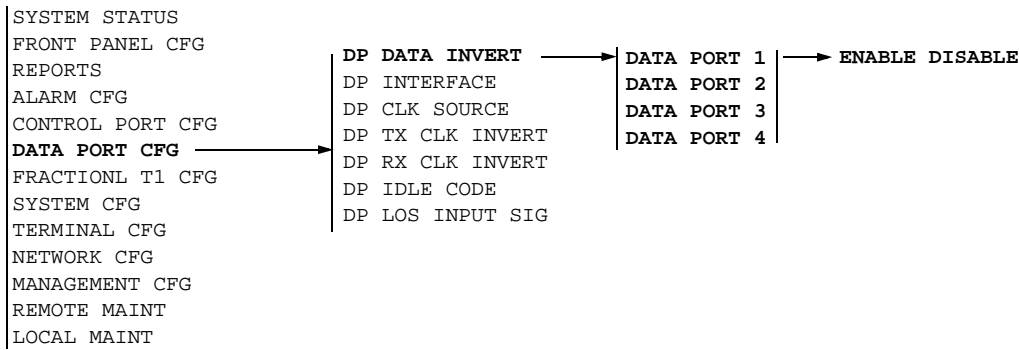
Using the command line

Use the following commands to enable or disable data inversion. You must have super-user or configuration privileges. The command syntax is:

- EDIn** Enable data inversion at data port *n*, where *n* is the number of the data port: 1 or 2 in a dual-port unit, or 1, 2, 3, or 4 in a quad-port unit.
- DDIn** Disable data inversion at data port *n*, where *n* is the number of the data port: 1 or 2 in a dual-port unit, or 1, 2, 3, or 4 in a quad-port unit.

Using the front panel

To enable or disable data inversion from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Select. DATA PORT 1 appears in the display.
- 5 Push Next or Previous until you see the appropriate data port in the display.
- 6 Push Select. ENABLE DISABLE appears. The currently configured value is blinking.
- 7 Push Next or Previous until the setting you want is blinking, then push Select.

Specifying the electrical interface of each data port

You can individually configure each data port interface to support either V.35 or EIA-530. Configure the port to support the interface requirements of the attached DTE device.

The default interface specification is V.35.

The interface specification is stored in the permanent nonvolatile configuration database.

Using the command line

Use the **INTF** command to specify the interface type. You must have super-user or configuration privileges. The command syntax is:

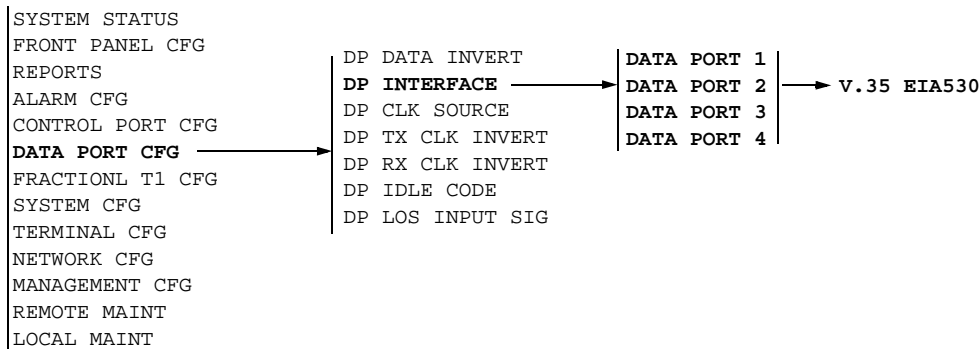
**INTF***n:cmd*

*n* Specify the data port number: 1 or 2 in dual-port units, 1, 2, 3, or 4 in quad-port units.

*cmd* Enter **V** for V.35 or **E** for EIA-530.

Using the front panel

To specify the interface types from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Next or Previous until DP INTERFACE appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.
- 6 Push Next or Previous until the appropriate data port appears in the display.
- 7 Push Select. V.35 EIA530 appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous until the setting you want is blinking, then push Select.



## Specifying data port clocking

You can specify the clock signal used to clock in transmit data at the data port. (Transmit data is data received at the data port from the DTE and transmitted to the network.) Two clock selections are available: internal or external.

- Internal clocking means that the transmit data is clocked by the data port's internal clock, which is derived from the DataSMART MAX system source clock.
- External clocking means that the transmit data is clocked by an externally supplied clock received on the data port.

The normal operation of synchronous serial data ports provides for three clock signals (see Figure 5):

- 1 The DCE supplies the receive (Rx) clock signal synchronized with the receive (Rx) data.
- 2 The DCE also supplies the transmit (Tx) clock signal. The DTE normally transmits its data synchronized to this signal. Most data terminal equipment uses this signal.
- 3 The external clock signal is generated by the DTE and is used in two different applications. The first application is when you are using the external clock signal for tail circuit timing of the T1 circuit. In this application, the external clock signal is supplied by the DTE equipment. (See [“Specifying the system clock” on page 44](#) for more information about tail circuit timing.)

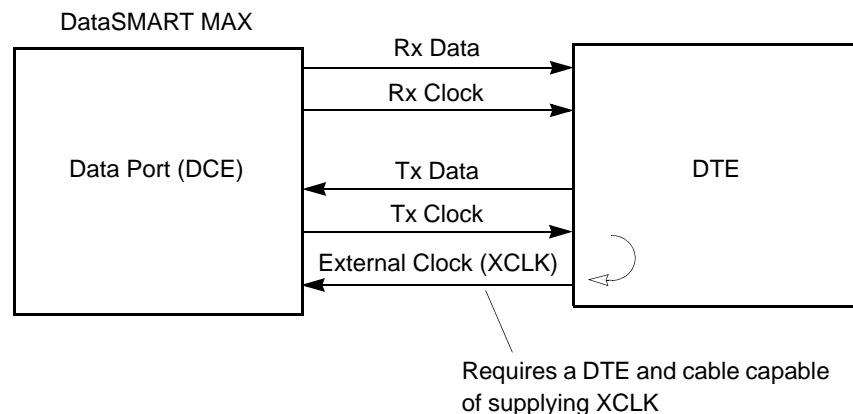
In the second application, the external clock signal is the Tx clock signal regenerated by the DTE and synchronized with the DTE's transmitted data. Usually you employ this option when you are receiving excessive data errors at the data port due to cable propagation delay. Propagation delay becomes a problem when you are using a long data cable (exceeding 50 - 100 feet) at high data rates. Propagation delay can cause significant phase shift between the Tx clock signal from the DataSMART MAX and the Tx data signal from the DTE.



### NOTE

*Not all data terminal equipment supports an external clock signal. You must have terminal equipment capable of supplying this signal, however, in order to use the DataSMART MAX unit's external data port clock option.*

**Figure 5—Clock signals at the data port**



The default data port clock is internal.

The data port clock setting is stored in the permanent nonvolatile configuration database.

### Using the command line

Use the **SCLK** command to specify the data port clock. You must have super-user or configuration privileges. The command syntax is:

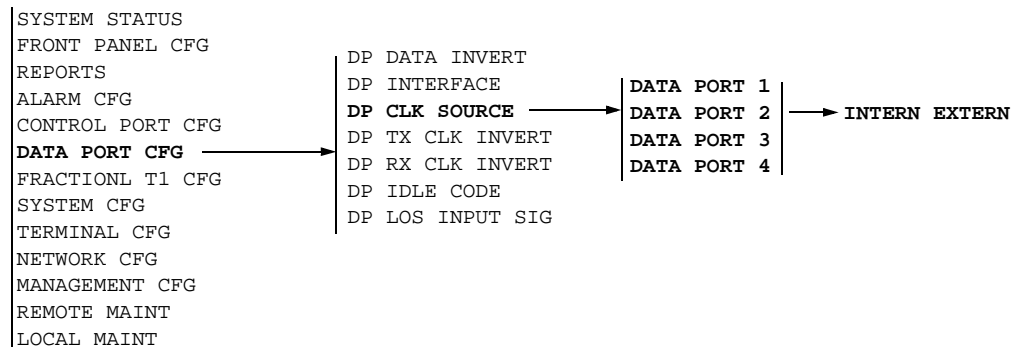
**SCLK***n:clk*

*n* Specify the data port number: 1 or 2 in dual-port devices, or 1, 2, 3, or 4 in quad-port devices.

*clk* Enter **E** to specify an external clock source, or enter **I** to specify the internal clock source.

### Using the front panel

To specify the data port clock from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Next or Previous until DP CLK SOURCE appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.
- 6 Push Next or Previous until the appropriate data port appears in the display.
- 7 Push Select. INTERN EXTERN appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous until the setting you want is blinking, then push Select.

Enabling/disabling  
transmit clock  
inversion

You can invert the transmit (Tx) clock signal and, by doing so, change the clock edge being used to sample transmit (Tx) data at the data port (refer back to Figure 5 on page 89). Transmit data is normally sampled on the falling edge of the transmit clock. If you invert the clock signal, data is sampled on the rising edge of the clock.

The inversion is done on the data port TCLK signal when internal source clocking is chosen and on the XCLK signal when external source clocking is chosen.

Sampling data on the falling edge of the clock is standard; you will seldom need to invert the clock. If the far-end is experiencing data errors, or if the cable connecting the DTE to the data port is long enough to cause undue propagation delays, you may need to invert the clock edge.

The default state is transmit clock inversion disabled.

The transmit clock inversion state is stored in the permanent nonvolatile configuration database.

Using the command line

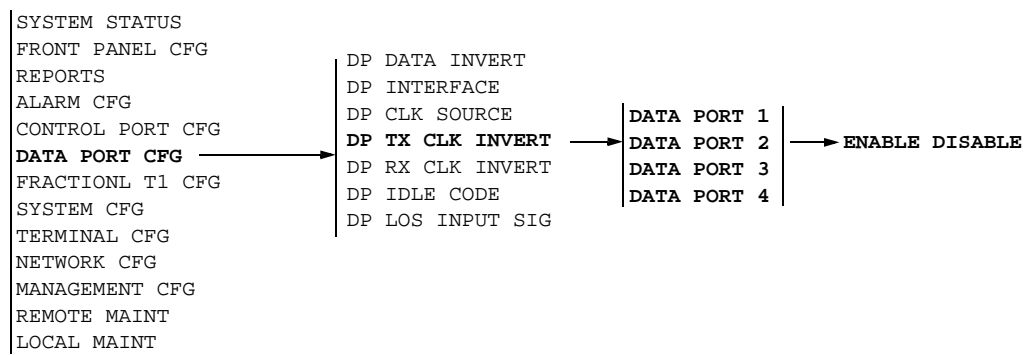
Use the **TCLK** command to invert the clock edge. You must have super-user or configuration privileges. The command syntax is:

**TCLK***n:cmd*

<i>n</i>	Specify the data port number: 1 or 2 in dual-port devices, or 1, 2, 3, or 4 in quad-port devices.
<i>cmd</i>	Enter <b>E</b> to enable clock inversion, or enter <b>D</b> to disable clock inversion.

Using the front panel

To enable transmit clock inversion from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Next or Previous until DP TX CLK INVERT appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.
- 6 Push Next or Previous until the appropriate data port appears in the display.

- 7 Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous until the setting you want is blinking, then push Select.

## Enabling/disabling receive clock inversion

You can invert the receive (Rx) clock signal and, by doing so, change the clock edge being used to clock the receive (Rx) data from the data port to the DTE (refer back to Figure 5 on page 89). Normally, receive data is changed on the rising edge of the receive clock. If you invert the clock signal, receive data is changed on the falling edge of the clock.

Changing receive data on the rising edge of the clock is standard; you will seldom need to invert the clock. If the local DTE is receiving clock slips or data errors, or if the cable connecting the data port and DTE is long enough to cause undue propagation delays, you may need to invert the clock edge.

The default state is receive clock inversion disabled.

The receive clock inversion state is stored in the permanent nonvolatile configuration database.

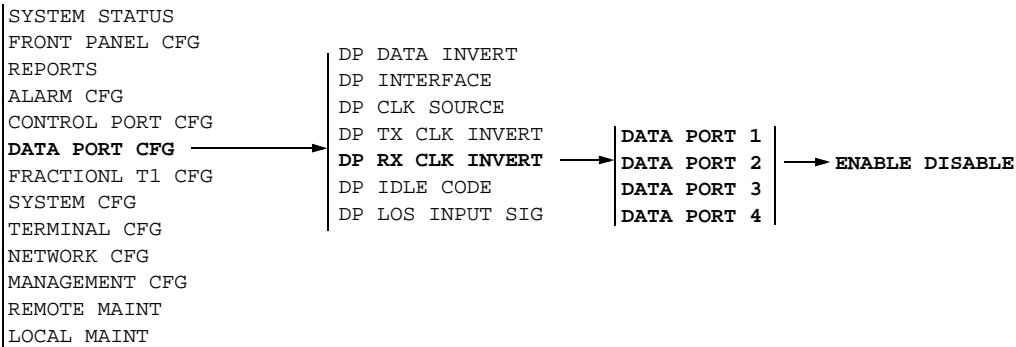
### Using the command line

#### **RCLKn:cmd**

- |            |   |
|------------|---|
| <i>n</i>   | Specify the data port number: 1 or 2 in dual-port devices, or 1, 2, 3, or 4 in quad-port devices. |
| <i>cmd</i> | Enter <b>E</b> to enable clock inversion, or enter <b>D</b> to disable clock inversion.           |

### Using the front panel

To enable receive clock inversion from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Next or Previous until DP RX CLK INVERT appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.
- 6 Push Next or Previous until the appropriate data port appears in the display.

- 7 Push Select. ENABLE DISABLE appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous until the setting you want is blinking, then push Select.

## Specifying the data port idle character

During certain alarm states and loopbacks, the DataSMART MAX outputs an idle character on the DS0 channels assigned to the data port. This idle character is transmitted to the network and to the DTE attached to the port. You can specify the value of this idle character as 0x7E, 0x7F, or 0xFF.

The default idle character is 0xFF. This value should work correctly for most equipment. Some equipment may require 0x7E or 0x7F. These characters were chosen because FF is normally sent out by T1 equipment. It is also an abort character in HDLC, as is 7F. (They both have more than six consecutive ones.) The character 7E is the flag character (idle) in HDLC.

The data port idle character is stored in the permanent nonvolatile configuration database.

### Using the command line

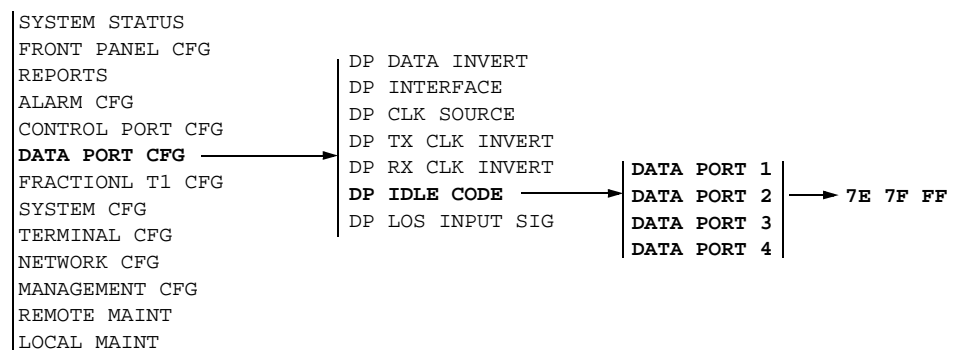
Use the **IDL** command to specify the idle character at the data port. You must have super-user or configuration privileges. The command syntax is:

**IDL***n:cmd*

- |            |   |
|------------|---|
| <i>n</i>   | Specify the data port number: 1 or 2 in dual-port devices, or 1, 2, 3, or 4 in quad-port devices. |
| <i>cmd</i> | Enter <b>7E</b> (0x7E), <b>7F</b> (0x7f), or <b>FF</b> (0xFF) to specify the idle character.      |

### Using the front panel

To specify the data port idle code from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Next or Previous until DP IDLE CODE appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.

- 6 Push Next or Previous until the appropriate data port appears in the display.
- 7 Push Select. 7E 7F FF appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous until the setting you want is blinking, then push Select.

## Setting up LOS (loss of signal) processing

You can specify which signals are monitored for LOS processing on each data port. You can monitor the RTS signal, the DTR signal, both signals, or neither signal.

When a data port LOS condition occurs, the DataSMART MAX fills the channels assigned to the data port with the idle character configured with the **IDL** command for transmission toward the network.

The default is to monitor RTS for LOS at the data port.

The data port LOS processing state is stored in the permanent nonvolatile configuration database.

### Using the command line

Use the **DPLOS** command to specify the signal(s) monitored for data port LOS. You must have super-user or configuration privileges. The command syntax is:

**DPLOS***n:cmd*

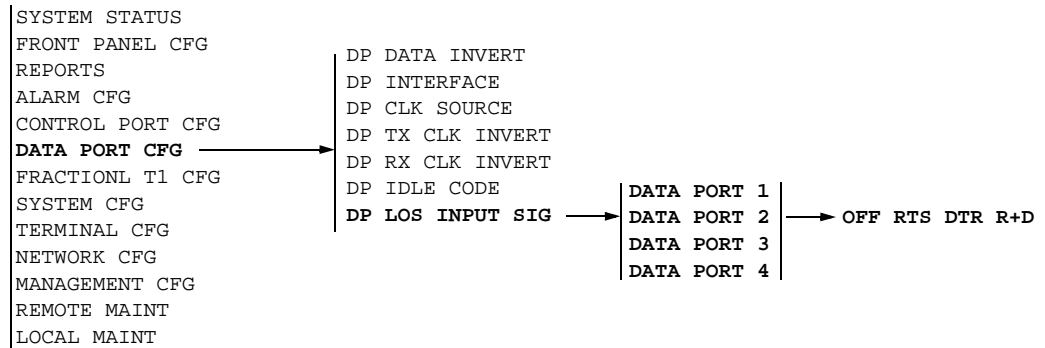
*n* Specify the data port number: 1 or 2 in dual-port devices, or 1, 2, 3, or 4 in quad-port devices.

*cmd* is one of the following:

- |          |  |
|----------|--|
| <b>R</b> | Monitor RTS for LOS. This should work correctly with most equipment. Some equipment or cables may need a different setting.                      |
| <b>D</b> | Monitor DTR for LOS.   |
| <b>B</b> | Monitor RTS and DTR for LOS. With this setting, the unit detects LOS if both RTS and DTR are low. If either signal is high, LOS is not detected. |
| <b>N</b> | Disable LOS monitoring. The DataSMART MAX ignores RTS and DTR at the port and assumes that the data port is connected and receiving valid data.  |

## Using the front panel

To specify the signals being monitored for LOS, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until DATA PORT CFG appears in the display.
- 3 Push Select. DP DATA INVERT appears in the display.
- 4 Push Next or Previous until DP LOS INPUT SIG appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.
- 6 Push Next or Previous until the appropriate data port appears in the display.
- 7 Push Select. OFF RTS DTR R+D appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous until the setting you want is blinking, then push Select.

---

## Assigning channels

The T1 line provides access to 24 DS0 channels on the network interface. You can configure the DataSMART MAX so as to connect some of these channels to data ports, some to a terminal interface, and leave other channels idle.

By default, for models with no terminal interface, all channels are assigned to idle. For add/drop models, all channels are assigned to the terminal interface.

You can assign channels using the command-line interface or the front-panel interface. You can completely configure the DataSMART MAX from the front-panel interface. There are some fundamental differences between the two methods.

- When you use the front-panel interface, the changes you make are loaded directly into hardware.
- When you use the command-line interface, you are actually editing a table which you then load into hardware in a separate step.

The DataSMART MAX has two tables, A and B, so that you can keep two separate configurations. This feature is useful at sites where, for instance, you have separate configurations for day-time and night-time traffic.

If you assign a channel configuration on the front panel, there is no way to later load it into one of the tables. If you make changes to the configuration using the front panel, it does not affect either of the tables.

### Rules for assigning channels

#### Rules for assigning data port channels

When assigning network interface channels to the data ports and the terminal interface, the channels for each data port must be grouped. Within the group, the channels can be contiguous or alternating. If the channels in the group are alternating, the intervening channels are assigned to idle.

For instance, if data port 1 had eight channels to assign, you could assign them in a single group of contiguous channels (1-8), but not two groups on contiguous channels (1-4 and 10-13). Or, if you wanted to use alternating channels, you could assign them to a single group of alternating channels (2, 4, 6, 8, 10, 12, 13, 14), but not to two groups of alternating channels (2, 4, 6, 8 and 14, 16, 18, 20).

The alternating channel configuration ensures that a circuit meets the ones density requirements when 64 Kbps is selected. In this configuration, the assigned channels are interleaved with channels filled with the idle code. The idle code **MUST** contain sufficient ones to keep the circuit synchronized. Note that the idle code is user-configurable (see the terminal interface menu), and if you are using it to fill alternating channels, make sure you select a code with sufficient ones. The idle code used in alternating channels configuration is defined by the TI menu idle code, not by the DP menu idle code.



#### NOTE

*Besides assigning the channels, you must also specify the data rate for the data port.*



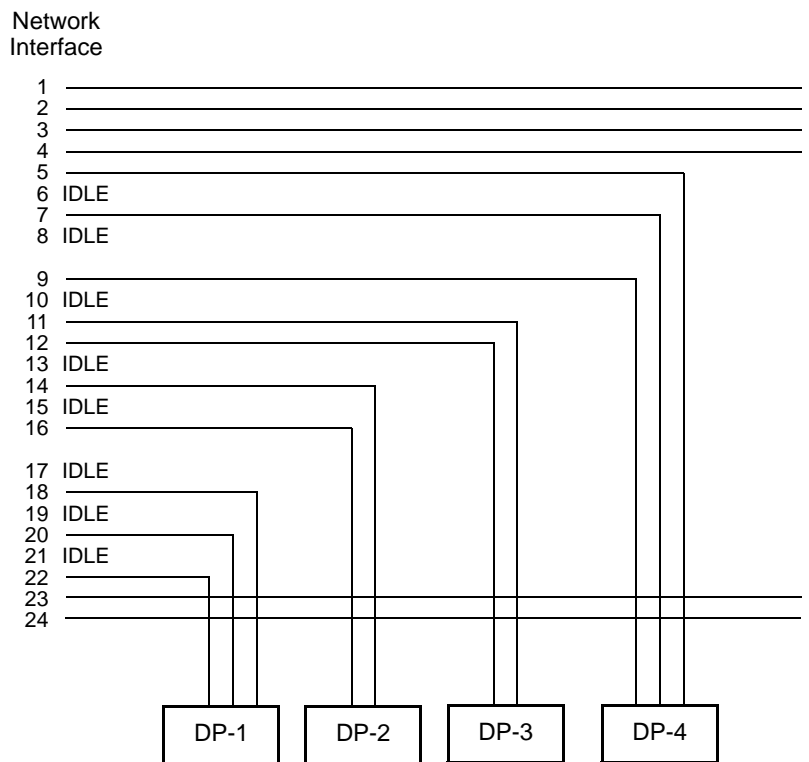
## Rules for assigning terminal interface channels

The three rules for channel assignments between the network interface and the terminal interface are:

- 1** The channel number on the TI side must match the channel number on the NI side. For instance, channel 1 on the TI side should be assigned to channel 1 on the NI side.
- 2** If equipment connected to the TI requires the A, B (super frame) signaling bits or the A, B, C, D (extended super frame) signaling bits to be passed through the unit, set the channel type to V (voice).
- 3** If the equipment connected to the TI requires a clear channel, set the channel type to D (data).

You do not need to group the TI channels in any special way, as is the case with data port channels. Also, if you use an alternating scheme, you can assign a single data port channel to a channel in between two TI channels.

The figure below shows a valid configuration for a DataSMART MAX with four data ports and a terminal interface.



## Assigning channels from the command line

You set channel bandwidth using the commands listed in the Fractional T1 Configuration menu. To display this menu, enter **FC**.

### FRACTIONAL T1 CONFIGURATION MENU

```
<table>DP<port>:<rate>[,<nicn>]
    - DP=Assign NI Channel Map for Data Port
    table A/B      - Tables A or B Containing Channel Assignment
    port  1 .. 4   - Data Port Number
    rate  56/64    - Channel Rate in 1000 bps
    nicn  1 .. 24  - NI Channel numbers assigned to Data Port or
    1,3,5,...     - Can be alternating DS0 channel numbers or
    1-24          - a contiguous range.

<table>NI<nicn>:<ticn>,<nicn>:<ticn>, ...
    - NI=Assign NI Channels to TI or IDLE
    table A/B      - Tables A or B Containing Channel Assignment
    nicn  1 .. 24  - NI Channel numbers
    ticn  V,D,I    - Voice/Data on TI Channel or I for Idle

CPAB / CPBA      - Copy A to B or B to A
LXA  / LXB       - Load and Execute Table A or B
TAV  / TBV       - View Table A or B
TXV              - View Executing Channel Assignment
```

The menu has commands for assigning channels, loading tables, viewing tables, and viewing the channel assignment currently in use.

There is also a command for copying one table to another, which is useful for creating two similar tables, or for making a backup of a table that you are about to edit.

### Assigning DS0 lines to a port

This command allows you to edit the data port channel assignments and the data rate. The command allows you make the changes in either table A or table B. Note that the command includes a syntax for assigning alternating channels.

You must have super-user or configuration privileges to use this command.

*tableDPport:rate[,nicn]*

<i>table</i>	Specify <b>A</b> or <b>B</b> to indicate which table you want to edit.
<i>port</i>	Specify the data port to which you are assigning channels: 1 or 2 in dual-port devices, or 1, 2, 3, or 4 in quad-port devices.
<i>rate</i>	Specify either <b>56</b> or <b>64</b> to indicate the data rate in kilobits per second.
<i>nicn</i>	Specify the NI channels that you want to assign to the data port, where <i>nicn</i> is one of the following: <ul style="list-style-type: none"> <li>A single channel number (for example, <b>11</b>).</li> <li>A range of channel numbers, delimited by a dash (for example, <b>2-8</b>).</li> <li>A series of odd or even channel numbers, delimited by a comma</li> </ul>

(for example, **7,9,11** or **10,12,14**).

The following example edits table A and assigns to port 2 a rate of 56 Kbps and channels 20 through 24, for an aggregate of 280 Kbps:

**adp2:56,20-24**

The next example allows you to change the data rate at a data port without entering the entire map for the port:

**adp2:64**

### Assigning network channels to the terminal interface or IDLE

Use this command to:

- assign network (NI) channels to the terminal interface (TI)
- idle out unused channels on the NI
- assign “voice” or “data” data to TI channels

Note that the assignments must be “straight across”; the NI channel must go to the TI channel of the same number.

You must have super-user or configuration privileges to use this command.

*table***NI***ni\_channel:[d,v,i]*

*table***NI***ni\_channel\_range:[d,v,i]*

*table***NI***ni\_single\_channel:[d,v,i]*

*table* Specify **a** or **b** to indicate which table you want to edit.

*ni\_channel\_range* Specify a range of NI channels to assign to the TI, delimited by a dash. For instance, **1-10** would assign NI channels 1 through 10 to TI channels 1 through 10. You can also use a range to set channels to idle. For instance, **1-10:i** would set channels 1 through 10 to idle. Another example: **11:20d,22-24:v** sets channels 11 through 20 to data, and channels 22 through 24 to voice.

*single\_channel:i* You can also set a single channel to idle. For instance, **3:i** sets NI channel 3 to idle.

You can specify none, one, or more of either *range* or *single*, delimited by commas.

Following are several examples of how to use this command. This example edits table B, setting all 24 channels to idle:

**bni1-24:i**

This example edits table B, setting NI channels 1- 4 to idle and NI channel 10 to TI channel 10:

**bni1-4:i,10:v**

This example edits table B, setting all NI channels to the corresponding TI channels configured for data, except for 10, which is set to voice:

**bni1-9:d,10:v,11-24:d**

**Viewing the contents of table A and B**

You can inspect the contents of the tables by using the **TAV** and **TBV** commands. You must have super-user or configuration privileges.

**TAV**                      Display the contents of table A.

**TBV**                      Display the contents of table B.

The **TXV** command shows the current assignments. **TXV** does not require any privileges to use.

**TXV**                      Display the current channel assignments on the DataSMART MAX.

To look at table A, for example, enter the **TAV** command from any prompt. The table A report will look something like the display shown on the next page. The report displays the mapping of NI channels in two different ways. The top of the report lists the ports in the left column and shows rate and all channels assigned to that port to the right. The bottom of the report lists every channel and shows its assignment and whether it is configured for idle, voice, or data.

The default assignments are: for DSUs, all channels are assigned to idle; for add/drops, all channels are assigned to the terminal interface.

VIEW TABLE A OF THE FRACTIONAL T1 CONFIGURATION

MAP	RATE	TOTAL	NI CHANNELS
TI	-	-	1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,16, 17,18,19,20,21,22,23,24
DP1	56	0	
DP2	56	0	
DP3	56	0	
DP4	56	0	
IDLE	-	-	

NI MAP	NI MAP	NI MAP	NI MAP	NI MAP	NI MAP	NI MAP	NI MAP
1:IDLE	2:IDLE	3:IDLE	4:IDLE	5:IDLE	6:IDLE	7:TI D	8:TI D
9:TI D	10:TI D	11:TI D	12:TI D	13:TI V	14:TI V	15:TI V	16:TI V
17:TI V	18:TI V	19:TI V	20:TI V	21:TI V	22:TI V	23:TI V	24:TI V

Field	Description
MAP	This identifies the port.
RATE	This tells you data rates, 56 or 64 Kbps, for each DS0 channel currently assigned to the data ports.
TOTAL	This displays the total bandwidth assigned to the data ports (where bandwidth is determined by multiplying the rate per channel by the number of channels assigned to the port).
NI CHANNELS	This lists channel assignments by ports.
NI MAP	This lists channel assignments by channel number.

Configuring the interfaces from a table

These commands load a configuration from a table into the hardware, which then operates as configured. You must have super-user or configuration privileges.

- LXA** Load configuration from table A.
- LXB** Load configuration from table B.

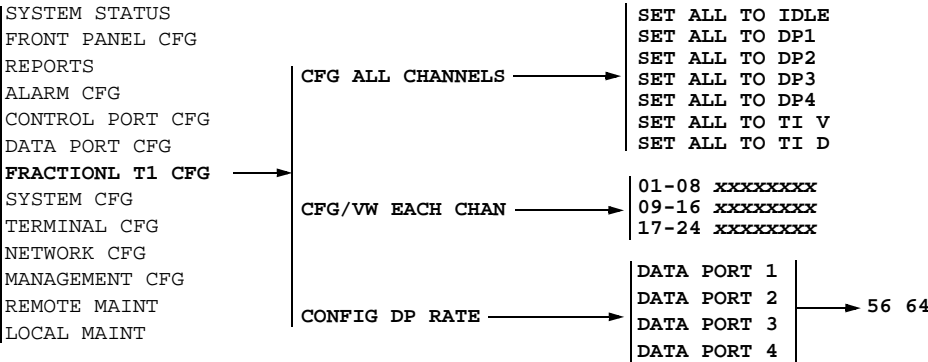
Copying one table into another

You can copy the contents of one table into the other table using the **CPAB** and **CPBA** commands. You must have super-user or configuration privileges.

- CPAB** Copies table A to table B.
- CPBA** Copies table B to table A.

Assigning channels from the front panel

The commands available for assigning channels from the front panel are shown below.



Using the CFG ALL CHANNELS command

This command is designed to simplify configuring channels from the front panel. For example, if you plan to configure your unit with most channels going to the terminal interface, you could use SET ALL TO TI. This assigns every channel to TI. Then you could use CFG/VW EACH CHANNEL to selectively change the other channels.

The steps for setting all channels are:

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRACTIONL T1 CFG appears in the display.
- 3 Push Select. CFG ALL CHANNELS appears in the display.
- 4 Push Select. SET ALL TO IDLE appears in the display.
- 5 Push Next or Previous until the desired setting appears in the display, then push Select.

## Using the CFG DP RATE command

Use this command to configure the data port DS0 channel data rate for each of the data ports.

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRACTIONL T1 CFG appears in the display.
- 3 Push Select. CFG ALL CHANNELS appears in the display.
- 4 Push Next or Previous until CONFIG DP RATE appears in the display.
- 5 Push Select. DATA PORT 1 appears in the display.
- 6 Push Next or Previous until the desired data port appears in the display.
- 7 Push Select. 56 64 appears in the display. The currently configured value is blinking.
- 8 Push Next or Previous to change to the desired value, then push Select.

## Using the CFG/VW EACH CHAN command

Use this command to assign or reassign from one to eight channels at a time to a data port, to the terminal interface, or to idle. You can also use this command to view the channel assignments from the front panel.



### NOTE

*The channel configuration display on the LCD is not updated dynamically. If another person is logged in the DataSMART MAX and changes a channel configuration while you are displaying the channel configuration on the LCD, you will not see the changes until the next time you select CFG/VW EACH CHAN.*

To view or change the channel assignments, follow these steps.

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRACTIONL T1 CFG appears in the display.
- 3 Push Select. CFG ALL CHANNELS appears in the display.
- 4 Push Next or Previous until CFG V/W EACH CHAN appears in the display.
- 5 Push Select. A display similar to the following appears, with the characters 01-08 blinking:

01-08 I I I I I I I I I I

The above example shows that channels 01-08 are set to idle. If channels 01-04 were assigned to the terminal interface, the display would show this:

01-08 V V V V I I I I I

The letters that indicate the channel settings can be V (voice), D (data), I (idle), or 1, 2, 3, or 4 (for the respective data port).

- 6 If you want only to view the channel settings, push Next or Previous to see channels 09-16 and 17-24. If you want to change a channel assignment, go to step 7.

- 7** To change a channel assignment, push Select. The channel range stops blinking and an underline appears under the first channel letter.
- 8** Push Next or Previous to move the underline to the letter that represents the channel you want to change. For instance, to change channel 2, the display should look like this:  
  
01-08 IIIIIIIII
- 9** Push Select. The underline disappears and the letter begins to blink.
- 10** Push Next or Previous to change the letter to the setting you want.
- 11** Push Select. The letter stops blinking and the underline reappears.
- 12** Repeat steps 8 through 11 until channels 01-08 are changed to the desired settings.
- 13** Push Escape. In the display “01-08” will begin to blink. You can now use Next or Previous to switch to ranges 09-16 and 17-24.
- 14** Push Next or Previous to switch to the other ranges as desired, and repeat steps 7 through 13.
- 15** When all channels are set as desired, push Escape. A query will ask “LOAD NEW CHANS?” Push Select to load the new channels, or push Escape to exit without making any changes.



## 5

*Performance monitoring*

---

This chapter describes how to monitor the performance of the incoming T1 circuits by using the various reporting facilities available from the DataSMART MAX command-line and front-panel interfaces.

Though this chapter describes different reports, learning to understand them is simplified by the fact that many are similar in format. For instance, all these reports are similar:

- User NI report
- User TI report
- Far-end report
- Carrier NI report

Because of the similarities of these reports, the easiest way to learn about them is to learn the most commonly-used report first, which is the User NI report. Descriptions of all other reports of the same type refer back to the description of the User NI report.

This chapter also describes three other reports:

- User NI Statistical Performance report
- User TI Statistical Performance report
- Alarm History report

This chapter is organized as follows:

- The first section shows how to access the various command-line reports.
- The next five sections show how to interpret the command-line reports.
- The final section shows how to access and interpret performance information from the front panel.

Though the reports described here contain some information about alarm status, the System Status report, described in Chapter 6, has more complete information. See [“Examining system status” on page 129](#).

**NOTE**

*You can also monitor performance of the incoming T1 circuits by using an SNMP network management system and accessing the DataSMART MAX MIBs.*

---

## Accessing the reports from the command-line

The Reports menu lists commands for accessing reports. To see the list, enter **R** at the command line.

```
REPORTS MENU

UNSR / UNLR    - User NI Short/Long Performance Report
UTSR / UTLR    - User TI Short/Long Performance Report
CNSR / CNLR    - Carrier NI Short/Long Performance Report
FESR / FELR    - Far End PRM Short/Long Performance Report

NSR:[z]        - User NI Statistical Performance Report
TSR:[z]        - User TI Statistical Performance Report
                z = Display Report then Zero Counts (Optional)
AHR            - Alarm History Report

PL:<len|style> - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                <style> = P (Page Break), M (More), or V (View)
```

To display any report, simply enter the appropriate command from the command line. You do not need any special privilege level.

Most reports have a long or short version. The long version differs from the short version only in that it includes a break-down of the performance information for the previous 24 hours, shown in 15-minute intervals.

### **TIP**

*For information on these and other reports, see the sections on interpreting performance reports starting on page 108.*

For example, use these commands to display the User NI reports.

**UNSR**                      Display the short version of the User NI report.

**UNLR**                      Display the long version of the User NI report.

### **Using the Z option with the NSR and TSR commands**

The NI and TI Statistical reports provide performance data similar to the NI and TI User reports, plus they provide in-service data about total errors counted at their respective interfaces. By using the **Z** option with the report command, either **NSR** or **TSR**, you can clear the error counts whenever the report is displayed. This way, the next time you display the report it will show just the errors accumulated since the last time you displayed the report.

The command syntax is:

**NSR [Z]**

**TSR [Z]**

**Z**                          Clears the in-service data from the report, once the report is displayed.

## Formatting the reports

The **PL** command formats all the reports, either for a printer or a terminal. You can set the page length and select either “page break” for output to a printer, or “more prompt” for output to a screen. A page length of 0 disables both page breaks and prompting.

By default, no page length is specified and page breaks and prompting are disabled. If you enter a page length, the command defaults to a “more prompt” (**M**) unless you specify “page breaks” (**P**).

The **PL** command syntax is:

**PL:***len/style*

<i>len</i>	Specify the page length as <b>0</b> , <b>20</b> ... <b>70</b> . 0 disables page breaks and prompting.
<i>style</i>	Specify <b>P</b> for “page break,” <b>M</b> for “more prompt,” or <b>V</b> to display the current settings without changing anything.

For example, to fit a report on a 22-line monitor, enter:

**PL:22:M**

Any time you change the length or style parameter, a display will show the state of the settings after the change.

## Clearing the performance database

At any time, you can clear the performance data and reset counters by executing the **ZALL** command (see [“Zeroing all counters” on page 50](#)). The **ZALL** command clears the data from all reports except the Carrier NI report and the Alarm History report.

Performance data is also cleared whenever you reset the date or time on the DataSMART MAX using the **ST** or **SD** commands (see [“Setting date and time” on page 40](#)).

You lose alarm history data if you cycle power to the DataSMART MAX. Performance data is stored for 10 hours nominal after a power loss.

If you use the **RSD** command to reset the DataSMART MAX to its defaults (see [“Resetting to default values” on page 51](#)), you lose the current alarm history data, performance data, and configuration settings. Use the **RSD** command with caution.

## Interpreting the User NI and the User TI reports

The DataSMART MAX monitors the received signal on a T1 line (both the network interface and the terminal interface) for a variety of different error conditions (see “[T1 alarms and signal processing](#)” on page 200 for descriptions of errored signal conditions). The DataSMART MAX logs the errors and then uses the log to determine quality of the 1-second interval during which the errors occurred.

For each time interval, the DataSMART MAX tallies the counts and displays the information in the reports. The reports also show the error conditions and whether or not an alarm was present.

The following figure shows an example of the User NI Short Performance Report (**UNSR**). The **UTSR** report is very similar.

```
KENTROX DataSMART MAX - USER NI SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000 NAME: PORTLAND,OR
DATE: MAR 14, 1995 TIME OF DAY: 00:27
STATUS CODES: C=CRC6, B=BPV, L=LOS, O=OOF, E=EER, A=AIS, Y=YEL,
              @=ALARM ACTIVE, T=TEST ACTIVE, N=NO POWER
SECOND OF INTERVAL: 757 OF 900 COMPLETED INTERVALS:96 OF 96
```

	EE	G.821 ES	BES	G.821 SES	G.821 UAS	CSS	G.821 DM	STATUS
CUR SEC	0	0	0	0	0	0	0	E @
PRE SEC	0	0	0	0	0	0	0	E @
CUR 15-MIN	3712	71	63	0	0	0	2	C E @
PRE 15-MIN	0	0	0	0	0	0	0	E @
CUR 24-HR	0	0	0	0	0	0	0	E @
03/13/95	2485	117	69	7	14	3	2	C O AY@
03/12/95	0	0	0	0	86400	0	0	L @
03/11/95	999999	86400	2139	0	0	72	1440	C E Y@
03/10/95	3296	459	192	17	313	3	7	C OE @T
03/09/95	4	1	1	0	0	1	0	C @
03/08/95	1	1	0	0	0	0	0	
03/07/95	1	0	0	0	0	1	0	

### Time intervals in the reports

The reports show the performance data for the current second, the previous second, the current 15-minute period, the previous 15-minute period, the current day, and the previous seven days.

Each day is broken into ninety-six 15-minute intervals. Interval one starts at 00:00 (midnight), interval two at 00:15, interval three at 00:30, and so on.

CUR 15-MIN refers to the performance data tabulated so far for the 15-minute interval. For instance, in the previous figure, the third row shows the performance for the 15-minute interval starting at 00:15 (notice that the time of day is 00:27).

Each 15-minute interval consists of 900 seconds. The field in the header labeled “SECOND OF INTERVAL” shows how many seconds into the interval the measurement extends. In the example, the data has been collected for 757 seconds of the current interval.

In a report, CUR 24-HR refers to a rolling 24-hour period. In other words, it is the previous ninety-six 15-minute intervals. The field labeled “COMPLETED INTERVALS” indicates whether or not the DataSMART MAX has been running for the full ninety-six intervals that make up a 24-hour day. Unless the DataSMART MAX was recently restarted, the completed intervals display should always read “96 OF 96.” The 24-hour count may show less than ninety-six 15-minute intervals if it was cleared within the last 24 hours.

The report also shows the performance data for each of the last seven days, if the DataSMART MAX has been powered up for seven days; otherwise, it shows the data collected since the DataSMART MAX was last powered up. For instance, if the DataSMART MAX has only been powered up for 48 hours, the report will only have a listing for two days, since only two days have completed so far. The unit retains data for a nominal 10 hours. If it was powered down for less than 10 hours, the old data is still available.

If one of the time intervals shows a row of dashes (-), that means that either the DataSMART MAX was powered down during that period or data has not yet been collected for that period.

A zero (0) indicates that the unit was collecting data and for that field the count was zero.

### Time intervals and the long report

The long report (use the **UNLR** or **UTLR** command) shows the same information as the short report and also includes performance data for each complete 15-minute interval in the current 24 hours (that is, the previous ninety-six 15-minute intervals). If not all of the 15-minute intervals are listed, it means the DataSMART MAX has not been on for 24 hours. A dash displayed in a field means that the unit was powered down for that period.

The following figure shows the additional information provided by the long version of the User NI report (**UNLR**).

TIME ACCUMULATED									
02:30	0	0	0	0	0	0	0		
02:15	0	0	0	0	0	0	0		
02:00	0	0	0	0	0	0	0		
01:45	0	0	0	0	0	0	0		
01:30	0	0	0	0	0	0	0		
01:15	0	0	0	0	0	0	0	E	@
01:00	2746	21	20	0	0	0	2	C	E @
00:45	104472	523	523	0	233	7	9	C LOEA	@
00:30	4009	76	68	0	0	0	2	C	E @
00:15	0	0	0	0	0	0	0	E	@

For each time interval there are eight types of performance measurements. These measurements are described below.

Field header	Definition
EE	<p>This field shows the number of error events (EEs) that have occurred, up to a maximum of 999,999. If the line uses ESF framing, the following error conditions cause a single EE to be counted:</p> <ul style="list-style-type: none"> <li>a transition to the LOS condition</li> <li>a transition to the AIS condition</li> <li>a transition to the OOF condition</li> <li>a controlled slip (sometimes referred to as a frame slip)<sup>1</sup></li> <li>a BPV error</li> <li>a CRC6 error</li> </ul> <p>If the line uses SF framing, an EE is the number of BPVs per second.</p>
ES	<p>This field lists the number of errored seconds (ESs) that have occurred. If the line uses ESF framing, an ES is any second that is not a UAS that contains:</p> <ul style="list-style-type: none"> <li>an LOS condition, or</li> <li>an AIS condition, or</li> <li>an OOF condition, or</li> <li>one or more CRC6 or BPV errors.</li> </ul> <p>If the line uses SF framing, an ES is any second with a BPV, LOS, AIS, or OOF.</p> <p>Note that controlled slips do not result in ESs (as per CCITT G.821 paragraph 1.8).</p> <p>Also note that when a single LOS, AIS, or OOF condition lasts for several seconds, it counts as a single EE, not as several ESs and SESs.</p>
BES	<p>This field lists the number of bursty errored seconds (BESs) that have occurred during the time interval, up to a maximum of 86,400.</p> <p>A BES is any second that is not a UAS that contains:</p> <ul style="list-style-type: none"> <li>no LOS, AIS, or OOF conditions, and</li> <li>between 2 and 319 (inclusive) EEs.</li> </ul>
SES	<p>This field lists the number of severely errored seconds (SESs) that have occurred, up to a maximum of 86,400. An SES is any second that is not a UAS that contains:</p> <ul style="list-style-type: none"> <li>an LOS condition, or</li> <li>an AIS condition, or</li> <li>an OOF condition, or</li> <li>320 or more EEs.</li> </ul>
UAS	<p>This field lists the number of unavailable seconds (UASs) that have occurred, up to a maximum of 86,400. A UAS state is declared when ten consecutive SESs occur. The ten SESs are subtracted from the SES count and added to the UAS count. Subsequent seconds are accrued to the UAS count until the UAS state is cleared. The UAS state is cleared when ten consecutive non-SESs occur. When that happens, the consecutive ten non-SESs are subtracted from the UAS count.</p>
CSS	<p>This field lists the number of controlled slip seconds (CSSs) that have occurred, up to a maximum of 86,400. A controlled slip second is any second that contains one or more controlled slips (see also the definition for ES). Note that CSSs are accumulated during unavailable seconds (UASs).</p>
<p><i>During any one second time period, the above error events can occur in various combinations. The possible combinations are: no errors; ES; CSS; ES and CSS and UAS; ES and BES; ES and BES and CSS and UAS; ES and SES; ES and SES and CSS and UAS; UAS, CSS and UAS.</i></p>	

Field header	Definition
DM	This field lists the number of degraded minutes (DMs) that have occurred, up to a maximum of 1,440. A DM is a sixty non-UAS and non-SES second period that contains 49 or more CRC6 or BPV errors (ESF framing) or 49 or more bipolar violations (SF framing).
STATUS	<p>This field shows the type of errored conditions that occurred during the time interval. The conditions are indicated by a single character as described below.</p> <p><b>B</b> For both ESF and SF, a “B” is displayed if a BPV occurs.</p> <p><b>C</b> If ESF is enabled, a “C” is displayed if a CRC6 error occurs.</p> <p><b>L</b> An LOS condition (but not necessarily an alarm) has occurred. (In a far-end report, “L” indicates a bipolar, or “line code” violation.)</p> <p><b>O</b> An OOF condition (but not necessarily an alarm) has occurred.</p> <p><b>E</b> An Excessive Error Rate (EER) alarm has occurred. This condition can occur only if the EE alarm is enabled.</p> <p><b>A</b> An AIS condition (but not necessarily an alarm) has occurred.</p> <p><b>Y</b> A yellow alarm has been detected.</p> <p><b>S</b> A controlled slip has occurred.</p> <p><b>@</b> There is an alarm state active on the DataSMART MAX.</p> <p><b>T</b> There is a (loopback) test active on the DataSMART MAX.</p> <p><b>N</b> The DataSMART MAX was without power.</p>

<sup>1</sup> A controlled slip is declared when the DataSMART MAX detects an accrued timing difference of exactly one frame between the transmitted and received data streams, resulting in the deletion or addition of a single frame in the received data stream.

## Interpreting the Far-end report

The **FESR** and **FELR** commands display the recent performance history of the received signal at the far-end network interface. The reports generated by the commands are similar to the User NI report. However, the data for the Far-end report is received from the remote device through Performance Report Messages (PRMs).

Because the Far-end reports are based on PRMs, PRM generation must be enabled in the far-end device, and the framing format of the T1 line must be ESF. (Use the **EPRM** command to enable PRM generation in the DataSMART MAX and use the **NESF** command to enable ESF framing format.)

The figure below shows an example of a short version of the Far-end report. Notice that it is the same as a User NI report except for the status codes described in the header and listed in the status column.

```
KENTROX DataSMART MAX - FAR END PRM SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000                      NAME: PORTLAND,OR
DATE: JAN 13, 1995                      TIME OF DAY: 10:53
STATUS CODES: C=CRC6, L=LCV, F=FRAME BIT ERR, E=SEVERE FRAME BIT,
              S=SLIP, P=PAYLOAD LOOP BACK, M=MISSED 4 PRM, N=NO POWER
SECOND OF INTERVAL: 495 OF 900 COMPLETED INTERVALS: 1 OF 96
```

	EE	G.821 ES	BES	G.821 SES	G.821 UAS	CSS	G.821 DM	STATUS
CUR SEC	319	1	1	0	0	0	0	C LF
PRE SEC	319	1	1	0	0	0	0	C LF
CUR 15-MIN	6776	59	59	0	0	0	1	C LFE M
PRE 15-MIN	-	-	-	-	-	-	-	
CUR 24-HR	-	-	-	-	-	-	-	

### Time intervals and the Far-end report

The method of dividing up time intervals for the Far-end report is the same as for the User NI report. See [“Time intervals in the reports” on page 108](#).

The following table describes the performance data displayed in the Far-end report.

Field header	Description
EE	<p>This first field lists the number of error events (EEs) that have occurred, up to a maximum of 999,999. Only CRC6 errors are used to calculate error events.</p> <p>The PRM message does not provide exact counts of CRC6 error events. Instead it uses 6 bits that indicate that the error rate fell within a certain range; then the highest number in the range (except for the last range, as noted below) is used as the error count in the Far-end report as follows:</p> <ul style="list-style-type: none"><li>1 CRC6 error-per-second counts as one EE</li><li>2 to 5 CRC6 errors-per-second count as 5 EEs</li><li>6 to 10 CRC6 errors-per-second count as 10 EEs</li><li>11 to 100 CRC6 errors-per-second count as 100 EEs</li><li>101 to 319 CRC6 errors-per-second count as 319 EEs</li><li>320 or more CRC6 errors-per-second count as 333 EEs</li></ul>
ES	<p>This field lists the number of errored seconds (ESs) that have occurred during the time interval, up to a maximum of 86,400. An ES is any second that is not a UAS that contains one or more CRC6 errors.</p>



Field header	Description
BES	This field lists the number of bursty errored seconds (BESs) that have occurred during the time interval, up to a maximum of 86,400. A BES is any second that is not a UAS that contains between 2 and 319 (inclusive) CRC6 errors.
SES	This field lists the number of severely errored seconds (SESs) that have occurred during the time interval, up to a maximum of 86,400. An SES is any second that is not a UAS that contains 320 or more CRC6 errors.
UAS	This field lists the number of unavailable seconds (UASs) that have occurred, up to a maximum of 86,400. A UAS state is declared when ten consecutive SESs occur. The ten SESs are subtracted from the SES count and added to the UAS count. Subsequent seconds are accrued to the UAS count until the UAS state is cleared. The UAS state is cleared when ten consecutive non-SESs occur. When that happens, the consecutive ten non-SESs are subtracted from the UAS count.
CSS	This field lists the number of controlled slip seconds (CSSs) that have occurred during the time interval, up to a maximum of 86,400. A controlled slip second is any second that contains one or more controlled slips (see also the definition for ES). Note that CSSs are accumulated during unavailable seconds (UASs).
<i>During any one second time period, the above error events can occur in various combinations. The possible combinations are: no errors; ES; CSS; ES and CSS and UAS; ES and BES; ES and BES and CSS and UAS; ES and SES; ES and SES and CSS and UAS; UAS and CSS.</i>	
DM	This field lists the number of degraded minutes (DMs) that have occurred during the time interval, up to a maximum of 1,440. A degraded minute is a sixty non-UAS and non-SES second period that contains 49 or more CRC6 errors (ESF framing) or 49 or more bipolar violations (SF framing).
Status	<p>This field shows the type of errored conditions that occurred during the time interval. The conditions are indicated by a single character as described below:</p> <p><b>C</b> A CRC6 error has been detected in the received T1 signal.</p> <p><b>L</b> A line code violation condition has occurred in the received network signal. A line code violation occurs when a bipolar violation that is not part of a zero-substitution code is received.</p> <p><b>F</b> A frame synchronization bit error has occurred in the received network signal. A frame synchronization bit error occurs when an error in the framing-bit-pattern is received.</p> <p><b>E</b> A severely-errored framing event has occurred in the received network signal. A severely-errored framing event occurs when two or more framing-bit-pattern errors occur within a 3-millisecond period.</p> <p><b>S</b> A controlled slip has occurred at the received network signal. A controlled slip event occurs when there is a replication or deletion of a T1 frame by the receiving network interface.</p> <p><b>P</b> A payload loopback is active on the network interface.</p> <p><b>M</b> No PRMs have been received for four or more consecutive seconds. Each PRM contains information for four consecutive seconds, and so no data is lost if up to three PRMs are missing.</p> <p><b>N</b> The near-end DataSMART MAX was without power.</p>

---

## Interpreting the Statistical reports

A Statistical report has two parts. The first part is a statistical summary of the recent performance history of the received signal. The second part is an in-service performance measurement of the received signal. The following figure shows an example of a Statistical report. The NI Statistical report (NSR) and TI Statistical report (TSR) differ only in that they monitor different interfaces.

```
KENTROX DataSMART MAX - USER NI STATISTICAL PERFORMANCE REPORT
ADDRESS: 00:00:000 NAME: PORTLAND,OR
DATE: JAN 6, 1995 TIME OF DAY: 02:52

      |----- G.821 -----|
      %AS    %EFS    %ES    %SES    %DM    %BES    %CSS
-----|-----|-----|-----|-----|-----|
CUR 15-MIN 100.00 100.00 0.0000 0.0000 0.0000 0.0000 0.0000
PRE 15-MIN 100.00 100.00 0.0000 0.0000 0.0000 0.0000 0.0000
CUR 24-HR  97.412 92.932 7.0679 0.0000 8.8435 6.9653 0.0797

START OF TEST: DATE: JAN 6, 1995
                TIME: 00:14
PERFORMANCE MEASUREMENT          COUNT
-----|-----|
ESF ERRORS                      188016
CRC6 ERRORS                     111215
OUT OF FRAME ERRORS              0
FRAME BIT ERRORS                 7471
BIPOLAR VIOLATIONS              0
CONTROLLED SLIPS                 7
YELLOW ALARM EVENTS              0
AIS EVENTS                      1344
LOSS OF FRAME EVENTS             985
LOSS OF SIGNAL EVENTS            6
LOSS OF POWER EVENTS            0
```

### The report's statistical summary

The statistical summary shows statistical percentages for the current 15-minute interval, the previous 15-minute interval, the current 24-hour interval, and each of the last seven days. These intervals are the same as those in the User NI or TI report; see [“Time intervals in the reports” on page 108](#) for a description of them.

The percentages are computed from the counts stored in the performance database for the User NI or TI report.

The statistical percentages are computed using the concept of an “available second”. In the formulas defined below, you will see the variable “Sec\_avail”. An available second is simply any second that is not an unavailable second:

$$\text{Sec\_avail} = \text{Sec\_total} - \text{UAS}$$

Specifically, the number of available seconds for any time period is simply the number of total seconds for the time period (900 for 15 minutes, 86400 for 24 hours) minus the number of UAS seconds. See [“UAS” on page 110](#) for a definition of an unavailable second.

Anytime “Sec\_avail” is zero for a time period and the formula for computing the percentage uses “Sec\_avail” in a denominator, a series of dashes is displayed as the result instead of a numerical value.

The following is a list of the seven fields in the statistical summary and the formulas used to compute their values.

Field header	Description
%AS	This field lists the percentage of available seconds (%AS) for the time interval. The formula for this statistic is: $\%AS = (\text{Sec\_avail} / \text{Sec\_total}) \times 100$
%EFS	This field lists the percentage of error-free seconds (%EFS) for the time interval. An error-free second is any available second that was not an errored second. The formula is: $\%EFS = ((\text{Sec\_avail} - \text{ES}) / \text{Sec\_avail}) \times 100$ where ES is the number of errored seconds for the time interval.
%ES	This field lists the percentage of errored seconds (%ES) for the time interval. The formula for this statistic utilizes ES, where ES is the number of errored seconds. The formula is: $\%ES = (\text{ES} / \text{Sec\_avail}) \times 100$ Note that the sum of %EFS and %ES should be 100%.
%SES	This field lists the percentage of severely errored seconds (%SES) for the time interval. The formula for this statistic utilizes SES, where SES is the number of severely errored seconds (using the same definition as for the User NI report). The formula is: $\%SES = (\text{SES} / \text{Sec\_avail}) \times 100$
%DM	This field lists the percentage of degraded minutes (%DM) for the time interval. The formula for this statistic utilizes DM, where DM is the number of degraded minutes (using the same definition as for the User NI report). The formula is: $\%DM = (\text{DM} / ((\text{Sec\_avail} / 60) \text{ rounded to next higher integer})) \times 100$
%BES	This field lists the percentage of bursty errored seconds (%BES) for the time interval. The formula for this statistic utilizes BES, where BES is the number of bursty errored seconds for the time interval (using the same definition as for the User NI report). The formula is: $\%BES = (\text{BES} / \text{Sec\_avail}) \times 100$
%CSS	This field lists the percentage of controlled slip seconds (%CSS) for the time interval. The formula for this statistic utilizes CSS, where CSS is the number of controlled slip seconds for the time interval (using the same definition as for the User NI report). The formula is: $\%CSS = (\text{CSS} / \text{Sec\_avail}) \times 100$

## The Statistical report's in-service performance measurement

The second part of the report displays counts of various error conditions in the received network signal. These are just raw counts, not percentages. The data for this display is kept in registers separate from the registers used for other reports. You can reset the counts at any time. Resetting the count does not affect performance information (including the information in the first part of the Statistical report). The error counts are useful for running an in-service test on the network line.

To run an in-service test on the NI or TI interface, use these steps:

- 1 Issue the **NSR** or **TSR** command using the **Z** option to clear (zero-out) the error counts. For example,

### NSR Z

This displays the Statistical report, showing the error counts at the time the command was issued, and then clears the error data.

- 2 Wait the desired time interval.
- 3 Issue the command again.

This displays the error counts accumulated since the time you cleared the error counts.

The figure below shows an example of an in-service performance measurement. The header shows the start of the test, which is the time that the error counts were last cleared. Below that are two columns, listing the type of error condition and a corresponding error count. The maximum value that may appear in any count field is  $2^{32}-1$  (4,294,967,295). When this limit is reached, the count wraps to zero (0).

```
KENTROX DataSMART MAX - USER NI STATISTICAL PERFORMANCE REPORT
ADDRESS: 00:00:000 NAME: PORTLAND,OR
DATE: JAN 6, 1995 TIME OF DAY: 02:52
```

	%AS	%EFS	G.821 %ES	%SES	%DM	%BES	%CSS
CUR 15-MIN	100.00	100.00	0.0000	0.0000	0.0000	0.0000	0.0000
PRE 15-MIN	100.00	100.00	0.0000	0.0000	0.0000	0.0000	0.0000
CUR 24-HR	97.412	92.932	7.0679	0.0000	8.8435	6.9653	0.0797

START OF TEST: DATE: JAN 6, 1995  
TIME: 00:14

PERFORMANCE MEASUREMENT	COUNT
ESF ERRORS	188016
CRC6 ERRORS	111215
OUT OF FRAME ERRORS	0
FRAME BIT ERRORS	7471
BIPOLAR VIOLATIONS	0
CONTROLLED SLIPS	7
YELLOW ALARM EVENTS	0
AIS EVENTS	1344
LOSS OF FRAME EVENTS	985
LOSS OF SIGNAL EVENTS	6
LOSS OF POWER EVENTS	0

## Interface Statistical report

Counts of the following error conditions are maintained and displayed in response to the **NSR** or **TSR** command:

- ESF Errors (ESF only)
- CRC6 Errors (ESF and SF)
- Out of Frame Errors (ESF and SF)
- Frame Bit Errors (ESF and SF)
- Bipolar Violations (ESF and SF)
- Controlled Slips
- Yellow Alarm Events: this event is a transition from the condition of “not receiving yellow” to the yellow condition.
- AIS Events: this event is a transition from the condition of “not receiving AIS” to the AIS condition.
- Loss-of-Frame Events: this event is a transition from the framed condition to the OOF condition.
- Loss-of-Signal Events: this event is a transition to the LOS condition.
- Loss-of-Power Events: this is the count of the number of times power to the DataSMART MAX has been lost.

---

## Interpreting the Alarm History report

The Alarm History report (use the **AHR** command) shows the last twenty alarm messages. The alarm messages in the report are the same messages sent to the control port device when the control port alarm messages are enabled and configured for ASCII format.

A message is added to the report every time an interface changes to a different alarm state. The “Alarm Cleared” message is not issued unless all alarms on that line are cleared. The report logs up to twenty messages, most recent first. Once the report reaches twenty messages, subsequent messages cause the oldest message to be dropped.

See [“Monitoring alarm messages” on page 128](#) for a full list of the types of alarms messages that can appear in this report and their meanings.

The alarm messages are always displayed in user format, regardless of the Alarm Message Format defined with the **EUM/ESM** commands in the Alarm Configuration Menu.

Alarm messages will always appear in the Alarm History report, even if alarm messages were disabled with the **DAM** command in the Alarm Configuration Menu.

Information in the Alarm History report is not cleared when an **ST**, **SD**, or **ZALL** command is executed. Only power cycling the DataSMART MAX or executing the **RSD**, Reset System to Default Values, command under the System Configuration menu (SC) will clear the Alarm History report.

An example of the Alarm History report is shown below.

```
SET ALM JAN.13,1995 10:52 NI EER PORTLAND,OR      addr = 00:00:000
CLR ALM JAN.13,1995 10:52 NI   PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:51 NI YEL PORTLAND,OR      addr = 00:00:000
CLR ALM JAN.13,1995 10:50 NI   PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:47 NI YEL PORTLAND,OR      addr = 00:00:000
CLR ALM JAN.13,1995 10:31 NI   PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:18 NI EER PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:18 NI OOF PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:18 NI EER PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:18 NI OOF PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:18 NI LOS PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:17 NI EER PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI YEL PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI EER PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI LOS PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI EER PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI OOF PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI AIS PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI OOF PORTLAND,OR      addr = 00:00:000
SET ALM JAN.13,1995 10:16 NI LOS PORTLAND,OR      addr = 00:00:000
```

---

# Interpreting the Carrier NI report

**TIP**  
*For the purpose of monitoring the NI performance, there is generally no reason to use the Carrier NI report. The same information is available in more detail in the User NI report.*

The Carrier NI report allows you to view the carrier’s version of the performance data of the NI signal received by the DataSMART MAX.

At many sites, the DataSMART MAX is at the point of demarcation on a T1 line between a carrier and a customer premise. Therefore, the DataSMART MAX keeps two sets of registers, both of which collect performance data on the unit’s signal received at the network interface: one set of registers for the customer and one set of registers for the carrier.

The customer can view the performance data collected in the customer registers by using the User NI report. The customer can also view the performance data collected in the carrier registers by using the Carrier NI report. The carrier accesses the data in the carrier registers from a remote device using the facility data link.

The customer cannot alter the data in the contents of the carrier’s registers (clear it, for instance), nor can the carrier alter the data in the customer’s registers.

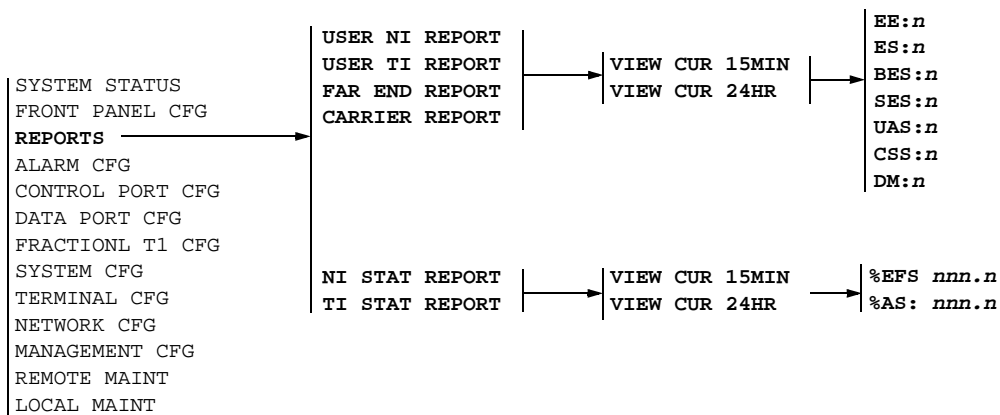
The format of the Carrier NI report is similar to that of the User NI report. The figure below shows a short version (using the **CNSR** command), though a long version (using the **CNLR** command) is available. The method of calculating the values in the report is per AT&T 54016.

KENTROX DataSMART MAX - CARRIER NI SHORT PERFORMANCE REPORT							
ADDRESS: 00:00:000				NAME: PORTLAND,OR			
DATE: JAN 6, 1995				TIME OF DAY: 00:31			
SECOND OF INTERVAL: 85 OF 900				COMPLETED INTERVALS: 2 OF 96			
	EE	ES	BES	SES	UAS	CSS	LOFC
	----	----	----	----	----	----	----
CUR SEC	0	0	0	0	1	0	0
PRE SEC	0	0	0	0	1	0	0
CUR 15-MIN	0	0	0	0	14	0	1
PRE 15-MIN	5036	93	85	0	0	0	0
CUR 24-HR	5371	95	85	2	47	1	1

# Accessing reports from the front panel

The front panel provides performance reports for the network interface (user and carrier version), the terminal interface, and the far end. It also provides a statistical version of the network interface and terminal interface data. The information available from the front panel is limited to the current 15-minute interval and the current 24-hour interval.

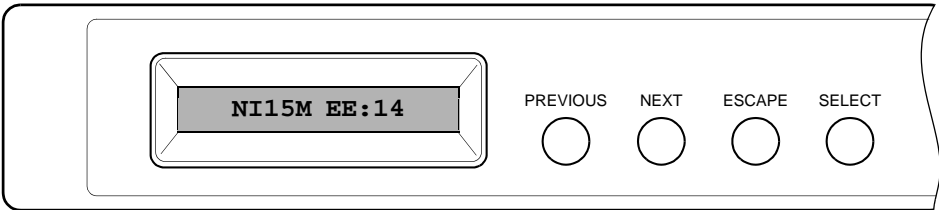
To view the performance reports from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until REPORTS appears in the display.
- 3 Push Select. USER NI REPORT appears in the display.
- 4 Push Next or Previous until you see the desired report in the display.
- 5 Push Select. VIEW CUR 15MIN appears in the display.
- 6 Push Next or Previous to switch to VIEW CUR 24HR, if desired.
- 7 Push Select to view the first report display.
- 8 Push Next or Previous to cycle through the report displays.

## Interpreting the LCD performance display

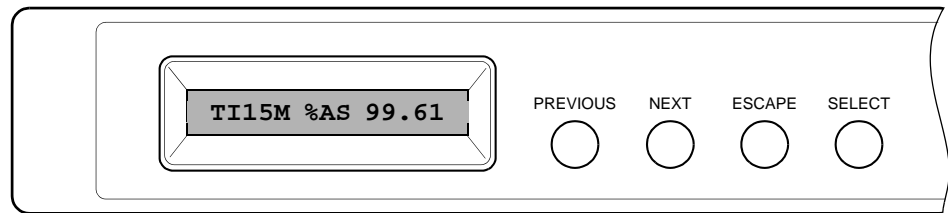
The figure below shows a situation in which the user has selected the User NI report for the current 15-minute time slice, as indicated by “NI15M” in the display. The display is positioned at the count for error events. Pushing Next or Previous will cycle through displays to show the counts for errored seconds, bursty errored seconds, and others.





The display is dynamic. The counts in the display update as new events occur. If the display is for the current 15-minute interval, the count resets to zero when a new 15-minute interval is entered (at 00:15, 00:30, 00:45, etc.). If the report shows the current 24-hour interval, the interval is rolling and always shows the totalled count for the previous ninety-six 15-minute intervals.

The display for the statistical information is similar to the performance reports. For example, the figure below shows the User TI report's percentage of available seconds for the current 15-minute time slice.



### Clearing the performance database

At any time, you can clear the performance data and reset counters by executing the **ZALL** command under the **SYSTEM CFG** menu (see [“Zeroing all counters” on page 50](#)). This clears the data from all reports except the Alarm History report.

Performance data is also cleared whenever you reset the date or time on the DataSMART MAX using **SD** (set date) or **ST** (set time) commands under the **SYSTEM CFG** menu (see [“Setting date and time” on page 40](#)).



## 6

*Troubleshooting*

This chapter describes how to troubleshoot the DataSMART MAX. It contains the following information:

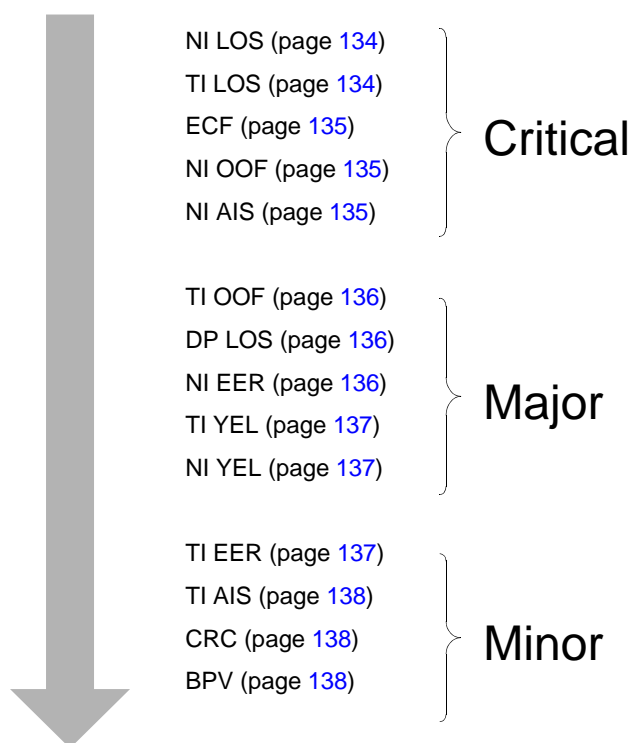
- How LEDs and alarm messages alert you when something is wrong
- How to find out the type of alarm and the interface at which it is occurring using either the front-panel or the command-line interface
- A list of all error conditions in the System Status report and suggestions of how to resolve them
- A description of how to use the DataSMART MAX diagnostic tools, including self test, loopbacks, and BERTs

***TIP***

*Always deal with critical alarms first.*

Following is a quick guide to the alarms generated by the DataSMART MAX and to the pages in this chapter that provide appropriate troubleshooting procedures for the alarms. The alarms are prioritized critical to minor. Always deal with critical alarms first.

**Figure 6—Troubleshooting the DataSMART MAX**



---

# Interpreting the front-panel LEDs

The front-panel LEDs provide an “on-site” way to alert you that the DataSMART MAX is experiencing abnormal conditions. When LEDs indicate abnormal conditions, you can use the front-panel LCD and keypad to get more detailed information about the problem (see page 130).

The figures on the following page show the information the LEDs provide during normal and abnormal conditions. On the pages following the figure is a table that provides detailed descriptions of how to interpret the LEDs.

## Selecting the data port to monitor

The data port LEDs on the left side of the front-panel show the status of only one data port at a time. You can switch these LEDs to monitor the desired data port.

### Using the command line

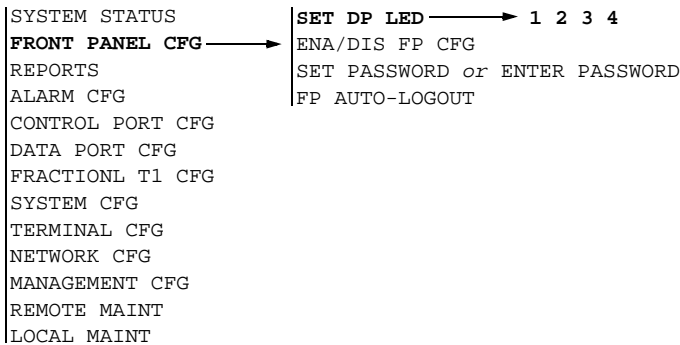
To switch the data port LEDs to a different data port, use the **DPLED** command. You do not need any special privilege level. The command syntax is:

#### DPLED*n*

*n* specifies the number of the data port: 1 or 2 in a dual-port device; 1, 2, 3, or 4 in a quad-port device.

### Using the front panel

To switch the data port LEDs to a different data port, use this sequence.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until FRONT PANEL CFG appears in the display.
- 3 Push Select. SET DP LED appears in the display.
- 4 Push Select. The data port numbers appear in the display with the current data port blinking.
- 5 Push Next or Previous to move to the desired port, then push Select.

Figure 7—LEDs when conditions are normal

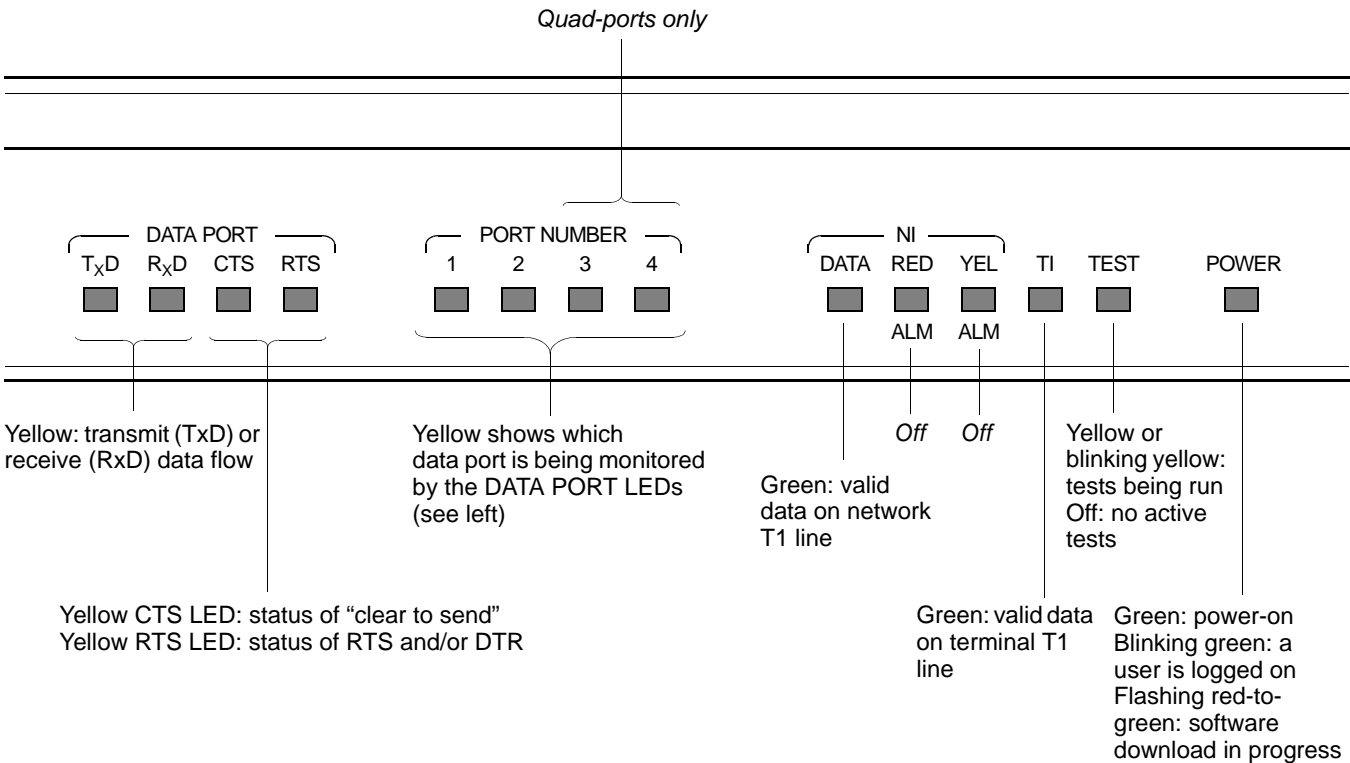
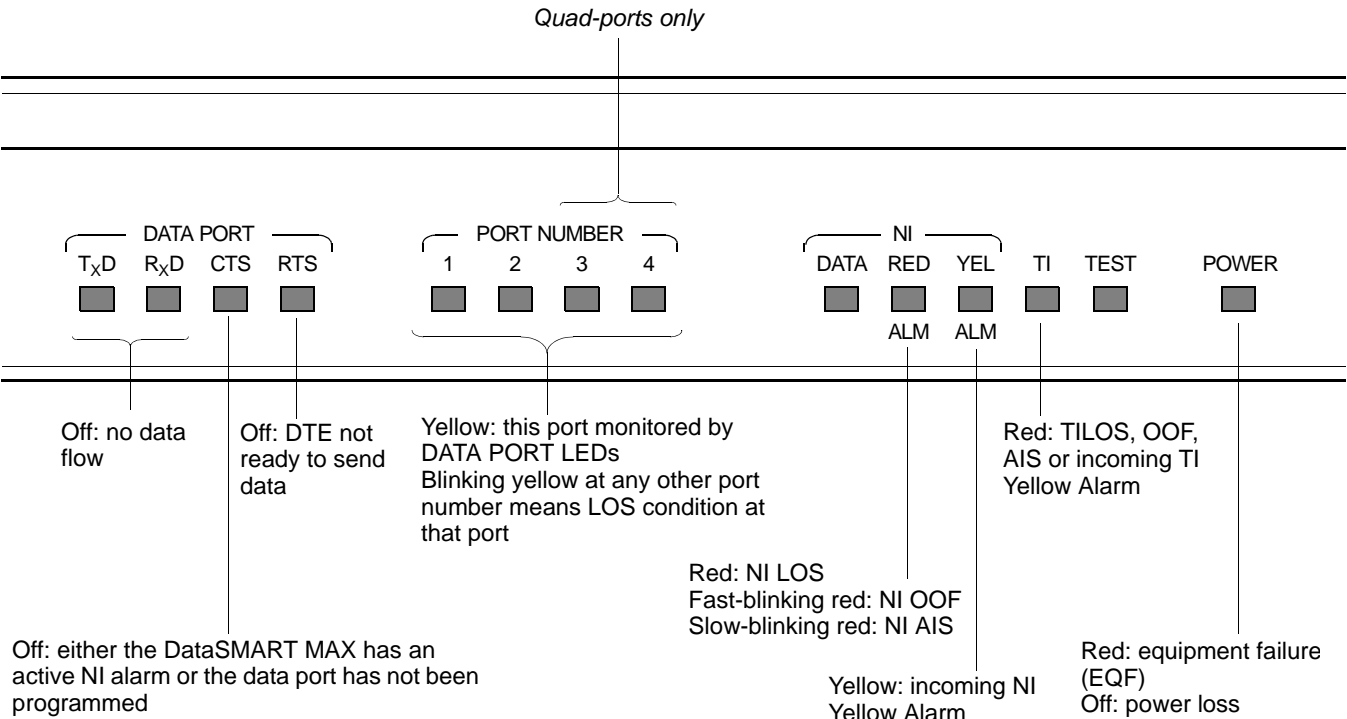


Figure 8—LEDs when conditions are abnormal



**Table 4—LED indicators and their meanings**

LED	Indicator	Condition
POWER	Green	Power is on, self-test successful.
	Green, blinking	A user is logged into the DataSMART MAX.
	Red-to-green, flashing	Software program is being downloaded.
	Red	Power is on, self-test failed.
	Off	No power is being received.
TEST	Yellow	Local loopback is set.
	Yellow, blinking	Test code or BERT is being run or remote loopback code has been sent.
NI DATA	Green	Valid framed signal is being received at the network interface.
NI RED	Red	LOS alarm. The T1 signal has been lost at the network interface.
	Red, blinking fast (5 times per second)	OOF alarm. The T1 signal is out-of-frame at the network interface. Some or all of the DS1 framing bits have been lost.
	Red, blinking slow (about once per second)	Incoming AIS alarm. The equipment on the other end is in test or alarm state.
NI YEL	Yellow	The equipment on the other end of the circuit is in OOF or LOS alarm.
TI	Green	Valid data is being received on the terminal T1 interface.
	Red	LOS, OOF, incoming AIS, or incoming yellow alarm at the terminal interface.
PORT NUMBER 1...4 <sup>1</sup>	Yellow	Only one of the PORT NUMBER LEDs can be yellow; it shows which data port is being monitored by the DATA PORT LEDs (see below). This LED never blinks.
	Yellow, blinking	The other three PORT NUMBER LEDs are either off or blinking. Blinking warns of an LOS condition at that data port, usually due to a loss of DTR or RTS (depending upon DPLOS configuration). These ports are <i>not</i> being monitored by the DATA PORT LEDs.

**Table 4—LED indicators and their meanings (continued)**

<b>LED</b>	<b>Indicator</b>	<b>Condition</b>
DATA PORT TxD	Yellow	Data is being transmitted (input) at the data port. Note that under normal conditions this LED may fluctuate in intensity.
DATA PORT TxD	Extended “off”	Spaces are being received at the data port. The spaces are transmitted to the network if RTS and CTS are high.
DATA PORT RxD	Yellow	Data is being received (output) at the data port. Note that under normal conditions this LED may fluctuate in intensity.
	Off	Zeroes are being output at the data port if RTS and CTS are on.
DATA PORT CTS	Yellow	Channels are assigned, and NI is not in alarm. The DataSMART MAX is ready to exchange data with the DTE.
	Off	This LED is off when it is not possible to transmit data out the data port. This may be because an NI alarm is present or the data port is not programmed or no channel is assigned.
DATA PORT RTS	Yellow	Request to send is asserted. The DTE is ready to send data to the DataSMART MAX, according to the conditions established by the DPLOS command.
	Off	The DTE is not ready to send data (per the conditions configured by the DPLOS command) or is not connected or channels are not assigned.

<sup>1</sup> Data ports 3 and 4 are available only on quad-port units.

---

## Monitoring alarm messages

The DataSMART MAX generates the alarm messages listed in Table 5 and outputs them at the control port. If you receive an alarm message, you should use the Status (**S**) command to get the details of the problem.

If two alarms occur simultaneously, the DataSMART MAX issues an alarm message for the higher priority alarm. When the higher priority alarm is cleared, the DataSMART MAX then issues the next lower priority alarm, if one is still present. The following table lists the alarms in the order of highest priority.

**Table 5—Alarms generated by the DataSMART MAX**

Alarm	Description
EQF	DataSMART MAX equipment failure.
ECF	External clock failure. If no clock, or if clock being received is significantly out of correct timing.
NI LOS	Loss of T1 signal at the network interface.
NI OOF	Out-of-frame T1 signal at the network interface. Some or all DS1 framing bits have been lost.
NI AIS	Incoming AIS (alarm indicator signal) at the network interface. Some device upstream of the network interface is in an LOS or OOF alarm state on the far side or in a test mode.
NI YEL	Incoming yellow alarm at the network interface. Some device upstream of the network interface is in an OOF or LOS alarm state on the near side.
NI EER	Excessive error rate detected on the T1 signal at the network interface.
TI LOS	Loss of the T1 signal at the terminal interface.
TI OOF	Out-of-frame T1 signal at the terminal interface. Some or all DS1 framing bits have been lost.
TI AIS	Incoming AIS (alarm indicator signal) at the terminal interface. Some device upstream of the terminal interface is in an alarm state on the far side.
TI YEL	Incoming yellow alarm at the terminal interface. Some device upstream of the terminal interface is in an LOS alarm state on the near side.
TI EER	Excessive error rate detected on the T1 signal at the terminal interface.
DP $n$ LOS	Loss of DTR and/or RTS at the specified ( $n$ ) data port.



# Examining system status

If the DataSMART MAX is in an alarm state or if you notice an abnormal condition, use the System Status report display to get more information. You can view the system status from the front-panel or the command-line interface. Both the front-panel display and the command-line report use the same status codes, which are explained in [Table 6 on page 130](#).

**TIP**  
For a discussion of how the DataSMART MAX transitions in and out of alarm states based on errored signal conditions, see “TI alarms and signal processing” on page 200.

The system status tells you the current condition of the DataSMART MAX, including any alarms that may be active as well as current — and possibly intermittent— signal conditions at the network interface, the terminal interface, and the data ports. Both the LCD status display and the command-line status display are dynamic and are updated as conditions change on the DataSMART MAX.

## Using the command line

To see the command-line display, enter **S** at the prompt. A screen similar to the one shown below appears. The display is updated once per second if the status changes, with the new status line added at the bottom. You exit the display by pressing Ctrl-C.

```
OPERATIONAL STATUS (^C TO EXIT)

JAN  4, 1995

TIME   SYSTEM   NI      TI      Data Ports
-----
        ALRM LPBK  IN  OUT  IN  OUT  DP1 DP2 DP3 DP4
-----
07:31  NLOS  -    LOS YEL  LOS AIS  -   -   -   -
```

Screen column	Description
TIME	This column shows the time of day (in 24-hour format) that the status line was generated.
SYSTEM ALRM	This column shows the highest priority state.
SYSTEM LPBK	This column shows if a loopback is active.
NI IN, NI OUT	These columns show the network interface RCV and XMT signal conditions.
TI IN, TI OUT	These columns show the terminal interface RCV XMT signal conditions.
Data Ports	These columns show the data port input signal conditions.

## Using the front panel

To view system status from the front panel, use these steps.

```
SYSTEM STATUS → ALM:- LB:-  
FRONT PANEL CFG NI RX:- TX:-  
REPORTS TI RX:- TX:-  
ALARM CFG DP 1:- 2:-  
CONTROL PORT CFG DP 3:- 4:-  
DATA PORT CFG  
FRACTIONL T1 CFG  
SYSTEM CFG  
TERMINAL CFG  
NETWORK CFG  
MANAGEMENT CFG  
REMOTE MAINT  
LOCAL MAINT
```

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Select to see the first system status display.
- 3 Push Next or Previous to cycle through the other status displays.

## Status codes

Table 6 explains the status codes and refers to a page for possible solutions.

**Table 6—Status codes on LCD**

Code	Description	Solution
<b>ALM — Alarm Status</b>		
—	No alarm exists.	Normal behavior.
ECF	External clock failure.	See <a href="#">page 135</a>
NLOS	Loss of the network input signal.	See <a href="#">page 134</a>
NOOF	The network input signal is out of frame.	See <a href="#">page 135</a>
NAIS	Incoming AIS (alarm indication signal) at the network interface.	See <a href="#">page 135</a>
NYEL	Incoming yellow alarm at the network interface.	See <a href="#">page 137</a>
NEER	Excessive error rate detected on the network input signal.	See <a href="#">page 136</a>
TLOS	Loss of the terminal input signal.	See <a href="#">page 134</a>
TOOF	The terminal input signal is out of frame.	See <a href="#">page 136</a>
TAIS	Incoming AIS (alarm indication signal) at the terminal interface.	See <a href="#">page 138</a>
TYEL	Incoming yellow alarm at the terminal interface.	See <a href="#">page 137</a>
TEER	Excessive error rate detected on the terminal input signal.	See <a href="#">page 137</a>
1LOS	Loss of DTR and/or RTS at data port 1.	See <a href="#">page 136</a>
2LOS	Loss of DTR and/or RTS at data port 2.	See <a href="#">page 136</a>
3LOS <sup>1</sup>	Loss of DTR and/or RTS at data port 3.	See <a href="#">page 136</a>

**Table 6—Status codes on LCD (continued)**

Code	Description	Solution
4LOS <sup>1</sup>	Loss of DTR and/or RTS at data port 4.	See <a href="#">page 136</a>
<b>LPBK — Loopback Status</b>		
—	No loopback is set.	Normal behavior.
RLLB	Code has been sent to set a remote line loopback.	Loopback test in progress.
RPLB	Code has been sent to set a remote payload loopback.	Loopback test in progress.
RDP <sub>n</sub>	Code has been sent to set remote data port loopback on data port <i>n</i> .	Loopback test in progress.
LLB	A line loopback is set on the local device.	Loopback test in progress.
LOC	A local loopback is set on the local device.	Loopback test in progress.
PLB	A payload loopback is set on the local device.	Loopback test in progress.
TLB	A terminal loopback is set on the local device.	Loopback test in progress.
DP <sub>n</sub>	A data port loopback is set on data port <i>n</i> of the local device.	Loopback test in progress.
DT <sub>n</sub>	A data terminal loopback is set on data port <i>n</i> of the local device.	Loopback test in progress.
<b>NI IN (Rx) — Network Input Status</b>		
LOS	Loss of the network input signal.	See <a href="#">page 134</a>
OOF	The network input signal is out of frame.	See <a href="#">page 135</a>
AIS	Incoming AIS (alarm indication signal) at the network interface.	See <a href="#">page 135</a>
YEL	Incoming yellow alarm at the network interface.	See <a href="#">page 137</a>
BPV	A bipolar violation has been detected on the network input signal. This applies only if the network signal is using SF framing.	See <a href="#">page 138</a>
CRC	A cyclic redundancy check error has been detected on the network input signal. This applies only if the network signal is using ESF framing.	See <a href="#">page 138</a>
QRS	A BERT running QRS test code is active at the network interface.	Normal behavior when a BERT is active.
324	A BERT running 3 in 24 test code is active at the network interface.	Normal behavior when a BERT is active.
247	A BERT running 2047 test code is active at the network interface.	Normal behavior when a BERT is active.
511	A BERT running 511 test code is active at the network interface.	Normal behavior when a BERT is active.
1'S	A BERT running all 1s test code is active the network interface.	Normal behavior when a BERT is active.
0'S	A BERT running all 0s test code is active at the network interface.	Normal behavior when a BERT is active.

**Table 6—Status codes on LCD (continued)**

<b>Code</b>	<b>Description</b>	<b>Solution</b>
—	Valid data is being received. No errors detected.	Normal behavior.
<b>NI OUT (Tx) — Network Output Status</b>		
YEL	Yellow alarm is being transmitted out the network interface. This occurs when LOS, OOF, or incoming AIS is detected at the network input signal.	See the entry in this table for Network input status codes LOS, OOF, or AIS.
QRS	QRS test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
324	3 in 24 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
247	2047 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
511	511 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
1'S	All 1s test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
0'S	All 0s test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
COD	The DataSMART MAX is in the process of setting or resetting a remote loopback.	Normal behavior.
—	Valid data is being transmitted out the network interface.	Normal behavior.
<b>TI IN (Rx) — Terminal Input Status</b>		
LOS	Loss of the terminal input signal.	See <a href="#">page 134</a>
OOF	The terminal input signal is out of frame.	See <a href="#">page 136</a>
AIS	Incoming AIS (alarm indication signal) at the terminal interface.	See <a href="#">page 138</a>
YEL	Incoming yellow alarm at the terminal interface.	See <a href="#">page 137</a>
BPV	A bipolar violation has been detected on the terminal input signal.	See <a href="#">page 138</a>
CRC	A cycle redundancy check error has been detected on the terminal input signal. This applies only if the terminal signal is using ESF framing.	See <a href="#">page 138</a>
—	Valid data is being received. No errors detected.	Normal behavior.

**Table 6—Status codes on LCD (continued)**

Code	Description	Solution
<b>TI OUT (Tx) — Terminal Output Status</b>		
YEL	Yellow alarm is being transmitted out the terminal interface. This occurs when incoming yellow alarm is detected at the network input signal.	Troubleshoot the alarm causing the output.
AIS	AIS (alarm indication signal) is being transmitted out the terminal interface. This occurs when LOS, OOF or incoming AIS is detected on the network input signal.	Troubleshoot the alarm causing the output.
—	Valid data is being transmitted out the terminal interface.	Normal behavior.
<b>Data Ports (DP<sub>n</sub>)</b>		
—	No bandwidth (channels) have been assigned to this data port.	Normal behavior.
CON	Bandwidth is assigned to the port, and the port is not in a LOS condition.	Normal behavior.
LOS	Bandwidth is assigned to the port, but a loss of DTR or RTS has been detected.	See page <a href="#">136</a>

<sup>1</sup> For quad-port models only.

---

## Troubleshooting tree

Bit errors received on the network port are the most common source of problems. The most common errors are:

- Wiring errors at the installation site
- Wrong type of wiring used for T1 line extension
- Incorrect configuration of equipment

The T1 circuit should be verified using the built-in DataSMART MAX loopbacks, test codes, and BERTs (bit error rate tests).

Here is a basic circuit verification test. Specific test methods will vary according to your application, but the basic principles remain the same:

- 1 Loop up the far-end equipment (see [“Using loopbacks” on page 142](#)).
- 2 Send a standard test code out the network interface (see [“Using test codes and BERTs” on page 150](#)).
- 3 Run BERT on that code to verify that all bits sent return unaltered.
- 4 Stop the BERT, remove the test code, and drop the far-end loop.

### Troubleshooting alarms

The best troubleshooting method is to start with the most serious alarm, find its cause and fix it, and then turn to the next most serious. The following alarm list is arranged from most to least serious. You may also want to use some of the diagnostic tools described later in this chapter.

#### NI LOS—critical

##### **If you receive a loss-of-signal condition at the network interface...**

An NI LOS condition occurs when the DataSMART MAX cannot detect a signal at its network interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART MAX network interface port and your T1 service provider’s equipment.
- If you built the cable on-site, check the cable connectors. A reversal of the transmit and receive pairs, or an open receive pair, can cause this condition.
- If the above appear to be okay, ask your T1 service provider to test your T1 line and correct any errors found.

#### TI LOS—critical

##### **If you receive a loss-of-signal condition at the terminal interface...**

A TI LOS condition occurs when the DataSMART MAX cannot detect a signal at its terminal interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART MAX terminal interface port and your CPE equipment.

- If you built the cable on-site, recheck the cable connectors. A reversal of the transmit and receive pairs, or an open transmit pair (CPE-to-DataSMART MAX), can cause this condition.



#### NOTE

*If you assign channels to the terminal interface but do not connect CPE equipment to the terminal interface, the unit will generate the TI LOS alarm.*

## ECF—critical

### If you receive an external clock failure (ECF) alarm...

An ECF alarm occurs when the DataSMART MAX is configured to use “External Master Timing,” but it cannot detect a clock signal at its Auxiliary port, either because the signal is not present or because the signal is significantly out of timing. To troubleshoot this condition:

- Verify whether or not the DataSMART MAX should really be set to External Master Timing. You should only use this timing option if a timing source is *not* provided by the T1 service. Controlled slips may occur if you set the DataSMART MAX to External Master Timing when a network clock is present. (External Master Timing is rarely used.)
- Check the cable connection between the DataSMART MAX Auxiliary port and your external clock source.
- Verify that your external clock source is powered up and configured correctly.
- Verify that your external clock source provides the correct type of clock signal, as shown in the DataSMART MAX specifications (see Chapter 8).

Refer to your *DataSMART MAX T1/FT1 Installation Guide* for instructions on how to properly connect an external clock cable.

## NI OOF—critical

### If the incoming signal at the network interface is out-of-frame...

An out-of-frame condition occurs when the framing type you have configured for the network interface does not match the framing type of the incoming T1 signal. Allowed framing types are ESF, SF, or Ericsson. To troubleshoot this condition:

- Change the framing type of the network interface (see [“Specifying NI framing format” on page 71](#)), or
- Ask your T1 service provider to change the framing type of your T1 line.

A highly errored incoming signal can also cause an OOF condition.

## NI AIS—critical

### If an alarm indication signal (AIS) is detected at the network interface...

An incoming AIS at the network interface indicates a problem with remote equipment on the T1 circuit. For example, the far-end equipment may not be connected or configured properly or is in a test mode, or the network interface unit (i.e., NIU or smart jack) may be in loopback, or your service provider may not have enabled your circuit yet. To troubleshoot this condition:

- Ask your T1 service provider to trace the source of the AIS signal.

## TI OOF—major

### If the incoming signal at the terminal interface is out-of-frame...

An out-of-frame condition occurs when the framing type you have configured for the terminal interface does not match the framing type of the signal being received at the terminal interface. Allowed framing types are ESF, SF, or Ericsson. To troubleshoot this condition:

- Change the framing type of the terminal interface (see [“Specifying TI framing format” on page 80](#)) or
- Change the framing type of the attached CPE equipment.

Note that a highly errored incoming signal can also cause an OOF condition. Check the description of TI EER.

## DP LOS—major

### If you receive a loss-of-signal indication at a data port...

A DP LOS condition occurs when the DataSMART MAX is not able to handshake as expected with an attached DTE device.

The DataSMART MAX can monitor two handshake lines on each data port: DTR and RTS. You can configure your DataSMART MAX to use either, both, or neither line as the DP LOS criteria (see [“Setting up LOS \(loss of signal\) processing” on page 94](#)). When the specified line goes low, the DataSMART MAX assumes that the DTE equipment has been disconnected or has failed. To troubleshoot this condition:

- Check the cable connection between the DataSMART MAX data port and the DTE.
- Verify that the cable is connected to the correct port at each end.
- Verify that you are using the correct cable for your application.
- Make sure that the DTE is powered up and that its serial port is activated.

Refer to your *DataSMART MAX T1/FT1 Installation Guide* for instructions on how to properly connect cables.

## NI EER—major

### If an excessive error rate is detected at the network interface...

The errors may be BPVs, CRC6 errors, or framing errors. There are several potential causes of an excessive error rate at the network interface. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting (see pages [64](#) and [65](#)).
- Make sure that you have correctly connected the cable between the DataSMART MAX network interface port and your T1 service provider's equipment. (Refer to your *DataSMART MAX T1/FT1 Installation Guide* for instructions on how to properly connect the cable.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure that you have configured the line coding of the network interface to match the line coding of your T1 line: either AMI or B8ZS. (See [“Specifying NI line coding” on page 73](#).)



- Make sure the system clock is configured correctly.
- If all the above appear to be okay, ask your T1 service provider to test your T1 line and correct any errors found.

## TI YEL—major

### If incoming yellow alarm is detected at the terminal interface...

An incoming yellow alarm at the terminal interface indicates that the CPE equipment attached to the interface is having a problem with the signal it is receiving from the DataSMART MAX. Most often, it is getting no signal at all. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART MAX terminal interface port and the CPE equipment. An open receive pair (DataSMART MAX TI port output to CPE input) can cause this condition.

## NI YEL—major

### If incoming yellow is detected at the network interface...

An incoming yellow condition at the network interface indicates that the far end equipment has a problem with the signal it is receiving from the DataSMART MAX. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART MAX network interface port and your T1 service provider's network interface unit (i.e., NIU or smart jack). An open transmit pair can cause this condition.
- If your application uses SF framing, and all 24 channels are used for data transmission, the actual data content can sometimes cause a "false yellow" condition. ESF framing is recommended for such applications. Other work-arounds may also be possible, depending upon your application.

## TI EER—minor

### If an excessive error rate is detected at the terminal interface...

The errors may be BPVs, CRC6 errors, or framing errors. There are several potential causes of an excessive error rate at the terminal interface. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting (see pages 64 and 65).
- Make sure that you have correctly connected the cable between the DataSMART MAX terminal interface port and your CPE equipment. (Refer to your *DataSMART MAX T1/FT1 Installation Guide* for instructions on how to properly connect the cable.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure that you have configured the line coding of the terminal interface to match the line coding of your CPE equipment: either AMI or B8ZS. (See "[Specifying TI line coding](#)" on page 81.)
- Make sure the system clock is configured correctly.

## TI AIS—minor

### If an alarm indication signal (AIS) is detected at the terminal interface...

An incoming AIS at the terminal interface may indicate that the CPE equipment attached to the terminal interface is not operational. To troubleshoot this condition:

- Check the programming of the CPE and make sure that its TI port is enabled.
- Check the wiring between the DataSMART MAX TI port and the CPE.
- Make sure that the framing type of the CPE matches the framing type configured for the terminal interface. Allowed framing types are ESF, SF, and Ericsson. (See [“Specifying NI framing format” on page 71.](#))

## BPV—minor

### If bipolar violations (BPVs) are detected at the network interface or the terminal interface...

A bipolar violation is an error in the normal polarity of received pulses. A bipolar violation occurs when two or more pulses of the same polarity appear in a row.

Bipolar violations are often caused by local problems with your T1 line. To troubleshoot this condition:

- Make sure that your T1 wiring consists of only *individually-shielded* twisted pairs.
- Check that all cable connections are secure and connected to the correct terminals. Refer to your *DataSMART MAX T1/FT1 Installation Guide* for instructions on how to properly connect cables.
- Make sure that you’ve set the line coding of the NI or TI interface to match the line coding of the T1 circuit: either AMI or B8ZS. A mismatch in line coding can often result in BPV errors.
- Make sure the system clock is configured correctly.

## CRC—minor

### If CRC6 (6-bit cyclic redundancy check) errors are detected at the network interface or the terminal interface...

CRC6 errors relate to ESF framing only. A CRC6 error indicates that bits were received in error in the previous extended superframe.

CRC6 errors are often caused by remote problems with your T1 line. To troubleshoot these types of errors:

- Make sure that you’ve set the line coding of the NI or TI interface to match the line coding of the T1 circuit: either AMI or B8ZS. This line code should be maintained throughout the connected circuit. A mismatch in line coding can often result in CRC6 errors.
- If the errors show up on the NI port, ask your T1 service provider to monitor the receive side of your line for CRC6 errors.
- If the errors show up on the TI port, check the configuration of the CPE.
- Make sure the system clock is configured correctly.

---

# Running the self-test diagnostics

At any time, you can initiate the DataSMART MAX self-test. The self-test verifies the functions of DataSMART MAX hardware circuitry. There will be a brief service interruption during the self-test.

When you execute the self-test, the DataSMART MAX automatically resets any loop-backs and deactivates any test code generation and bit error rate tests (BERTs). It does not clear the performance database, nor does it log you out of the system.

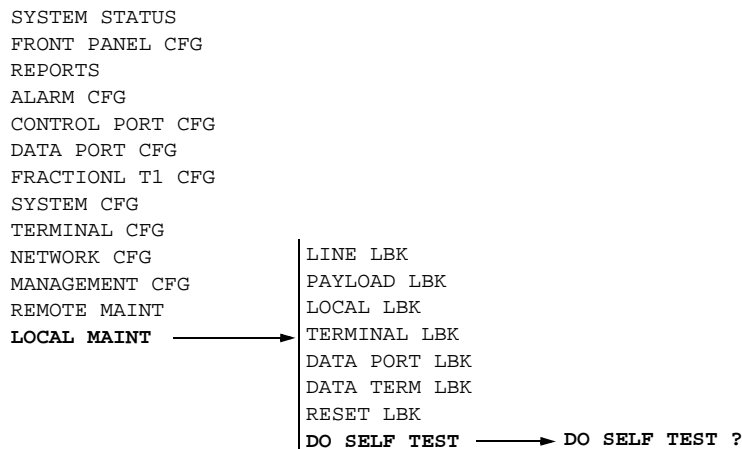
You cannot activate the self-test if you have logged into the DataSMART MAX remotely through the **ARC** command. The self-test would break your remote login connection.

## Using the command line

To initiate self-test from the command line, enter the **DST**. You must have super-user, configuration, or maintenance privileges.

## Using the front panel

To initiate self-test from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until LOCAL MAINT appears in the display.
- 3 Push Select. LINE LBK appears in the display.
- 4 Push Next or Previous until DO SELF TEST appears in the display.
- 5 Push Select. A query asks if you really want to start the self test. Push Select.
- 6 When the test is complete, the results appear in the display.

## Self-test error messages

The following messages announce problems discovered by the self-test. The message format differs slightly depending on whether the messages are sent to the LCD front-panel display or to the command line.

Contact our Technical Support organization if the self-test returns a “fail” condition.

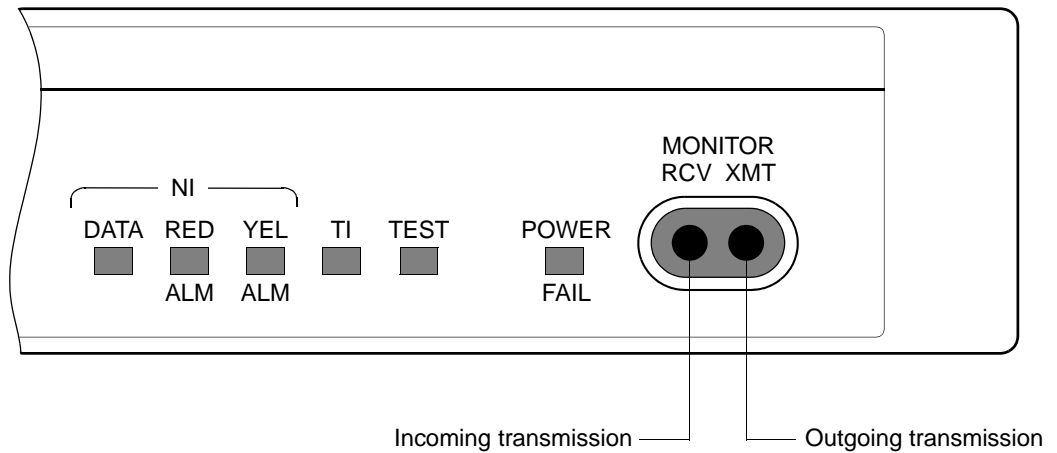
LCD front-panel display	Command-line display
SELF TEST PASSED	SELF TEST PASSED
RTC TEST FAILED	RTC TEST FAILED
FLASH ID FAIL	FLASH ID FAIL
FLASH SUM FAIL	FLASH SUM FAIL
EPROM ID FAIL	PROGRAM WORD FAIL
EPROM SUM FAIL	PROGRAM CHECK SUM FAIL
RAM ERR<hex address>	RAM TEST FAILED AT ADDR:<hex address>
RAM CSUM FAILED	RAM CHECK SUM FAILED
RAM PATRN FAILED	RAM PATTERN TEST FAILED
NI R/W TEST FAIL	NI READ/WRITE TEST FAILED
CGD DETECT FAIL	CGD DETECTION TEST FAILED
CGD DATA FAIL	CGD BIT ERROR RATE TEST FAILED
NI DATA FAIL	NI DATA TEST FAILED
TI R/W TEST FAIL	TI READ/WRITE TEST FAILED
TSA/DP<port number>FAIL	DATA PORT<port number>TEST FAILED

---

## Using the network signal jacks

The DataSMART MAX provides two non-intrusive monitor jacks on its front panel. You can attach standard T1 test equipment to these jacks and monitor incoming (RCV) and outgoing (XMT) T1 signal transmissions. The jacks are bantam-type.

20dB signal loss/protection is provided to isolate the test equipment from the T1 circuit.



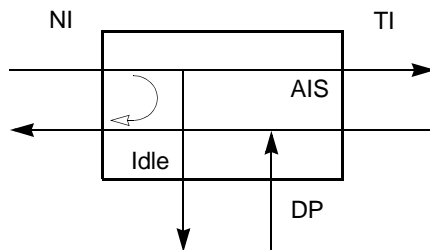
---

## Using loopbacks

The DataSMART MAX provides six loopbacks to support line segment testing. Line segment testing allows you to probe the T1 circuit to isolate where data flow is being corrupted or disrupted.

You can set all loopbacks locally, in your near-end device. You can also set the line, payload, and data port loopbacks remotely, in a far-end device. If you set a loopback in a far-end device, you can then use the DataSMART MAX to run bit error rate tests (BERTs) to test the T1 signal.

### Line loopback

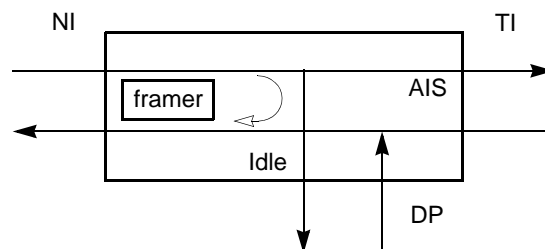


The line loopback allows the carrier (or a far-end device) to test the T1 signal at the DataSMART MAX network interface. When set in a line loopback, the DataSMART MAX loops the incoming T1 signal back to the network. The T1 signal does not penetrate the DataSMART MAX and so does not pass through the DataSMART MAX framer. The signal, including all line coding errors, is returned to the network unaltered and the carrier can test the looped signal for errors.

Once the line loopback is set, the incoming network signal is interrupted, and so the DataSMART MAX outputs idle characters at the data ports and AIS at the terminal interface.

You can set the line loopback locally (see page 146), or you can set it remotely in a far-end device (see page 148).

### Payload loopback



#### **TIP**

*You can also use a bi-directional BERT to isolate T1 line problems. See page 150.*

By testing the T1 signal through a line loopback as described earlier, the carrier (or the far-end device) can determine if there are problems in the network line. What they cannot determine, however, is whether the problems are occurring on the input or output side of the looped line. To further isolate the source of the problems to one side of the line or the other, you can change from a line loopback to a payload loopback.

Payload loopback is the same as line loopback, except that the signal passes through the DataSMART MAX framer before being looped back. The framer strips out BPV errors and recalculates CRC (for ESF framing format) but does not alter the payload data.

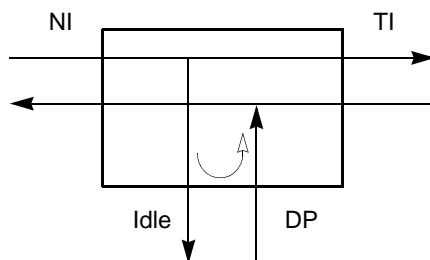
The condition of the returned signal indicates the cause of the problem:

- The line is okay if the returned signal contains no bit pattern errors, no BPVs, and no CRC6 errors.
- The problem is outbound if the returned signal contains pattern bit errors, but no BPVs or CRC6 errors.
- The problem is inbound and at the remote end if the returned signal contains pattern bit errors and CRC6 errors, but no BPVs.
- The problem is inbound and at the local end if the returned signal contains pattern bit errors, CRC6 errors, and BPVs.
- The problem is probably a remote clock slip if the returned signal contains pattern bit errors and is bursty, but contains no BPVs and no CRC6 errors.

Once the payload loopback is set, the incoming network signal is interrupted, and so the DataSMART MAX outputs idle characters at the data ports and AIS at the terminal interface.

You can set the payload loopback locally at the request of the carrier or a far-end site (see page 146), or you can set it remotely in a far-end device (see page 148).

## Data port loopback

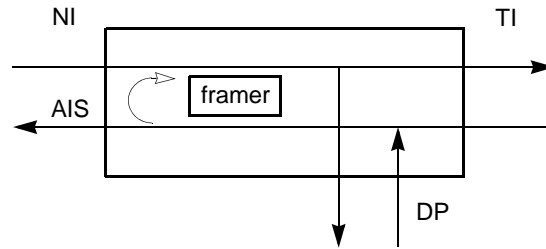


The data port loopback allows the carrier (or a far-end device) to examine the fractional channels assigned to a given data port. When set in a data port loopback, the DataSMART MAX receives the T1 signal at the network interface, distributes the fractional channels as assigned to the data port, then loops the channels back to the network. It does this without affecting the rest of the received payload. Normal transmission occurs at all other data ports and at the terminal interface.

Once the data port loopback is set, transmission at the specified data port is interrupted. The DataSMART MAX sends idle characters out the port to notify the connected terminal device.

You can set the data port loopback locally to facilitate testing with the carrier or a far-end site (see page 146), or you can set it remotely in a far-end device (see page 148).

## Local loopback



### **TIP**

*The local loopback is similar to a “hard” loopback set at the network interface.*

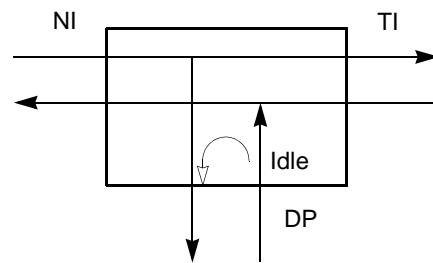
The local loopback allows you to verify if the DataSMART MAX is adding and dropping channels correctly. When set in this loopback, the DataSMART MAX “adds” all the incoming channels to the T1 bit stream, but instead of outputting the bit stream to the network, it loops the bit stream back from the network interface and drops out the channels to their respective data ports and/or terminal interface. By attaching terminal devices capable of monitoring the looped signals, you can verify that the correct channels are being returned to the correct ports.

When the DataSMART MAX is set in a local loopback, the outgoing T1 signal at the network interface is interrupted. The DataSMART MAX outputs AIS at the network interface.

The framer strips out BPV errors and recalculates CRC (for ESF framing format) but does not alter the payload data.

You can only set a local loopback in your local DataSMART MAX (see page 146); you cannot set it remotely.

## Data terminal loopback



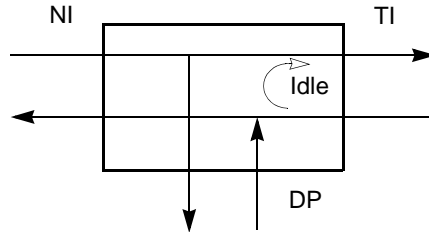
Typically, you use the data terminal loopback to verify the cabling between the data port and the attached DTE device. You can also monitor the looped signal for errors at the DTE.

The data terminal loopback allows you to loop the incoming signal at a specified data port. When set in this loopback, the DataSMART MAX loops the incoming signal back to the DTE device sending the signal. The signal does not penetrate the DataSMART MAX. The signal, including all line coding errors, is returned to the DTE device unaltered.



When set in a data terminal loopback, the DataSMART MAX inserts an idle character into the channels assigned to the data port. Normal activity continues at the network interface, at the terminal interface, and at all other data ports. You can only set a data terminal loopback in your local DataSMART MAX (see page 146); you cannot set it remotely.

## Terminal interface loopback



Typically, you use the terminal interface loopback to verify the cabling between the terminal interface and the CPE. You can also attach a test set to the terminal interface, send test codes, then run bit error rate tests on the looped signal.

The terminal interface loopback allows you to loop the incoming T1 signal at the terminal interface in add/drop devices. When set in this loopback, the DataSMART MAX loops the incoming T1 signal back to the CPE attached to the terminal interface. The signal does not penetrate the DataSMART MAX. The signal, including all line coding errors, is returned to the CPE unaltered.

When set in a terminal interface loopback, the DataSMART MAX inserts an idle character into channels assigned to the terminal interface. Normal activity continues at the network interface and at all data ports.

You can only set a terminal interface loopback in your local DataSMART MAX (see page 146); you cannot set it in a remote device.

# Setting and resetting loopbacks in your local device

You can set and reset loopbacks in your local device from the command line or the front panel. Only one loopback, either local or remote, may be set at one time. You cannot set a loopback if another loopback is already active, if test code is being transmitted, or if a BERT is active.

If you have logged into the DataSMART MAX via the **ARC** command, the DataSMART MAX *does not* allow you to set any loopback because loopbacks can potentially break the FDL link. The DataSMART MAX *does* allow you to set the line, payload, and data port loopbacks via Telnet. However, if you are accessing the DataSMART MAX via a SLIP connection and are communicating to it via the T1 payload, be aware that these loopbacks could potentially break the SLIP connection by breaking the T1 payload.

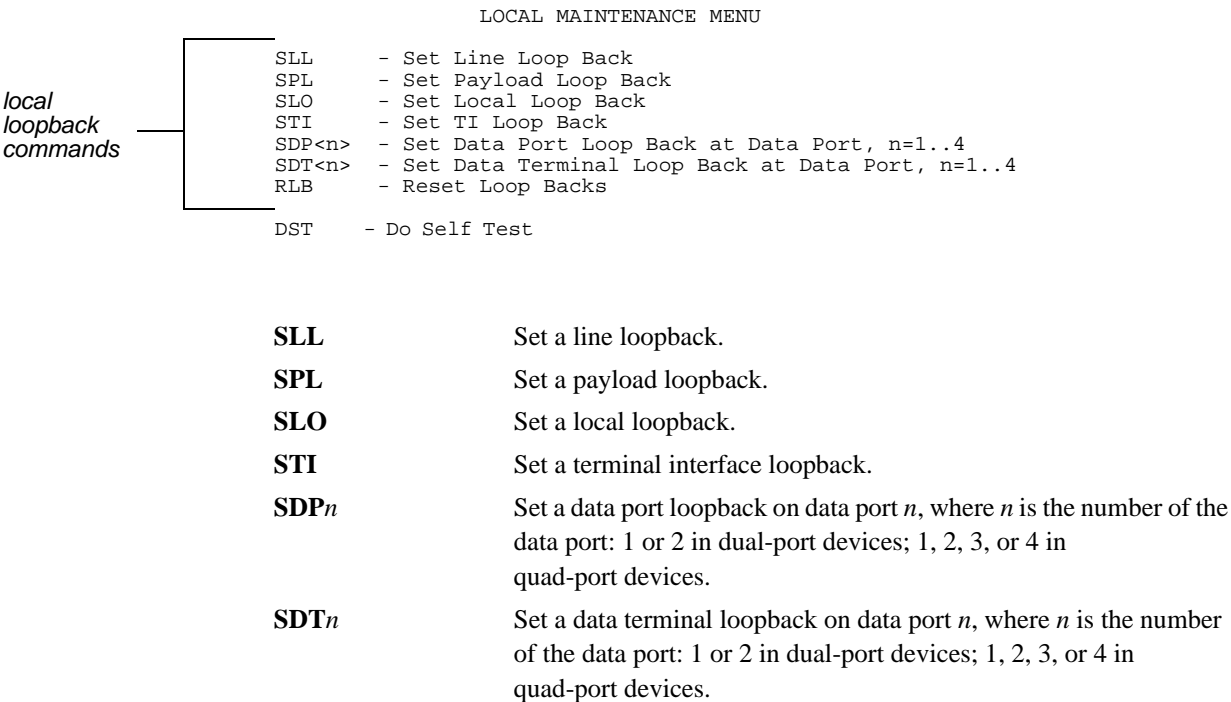


## NOTE

*A far-end device can set your local device in line, payload, or data port loopback by sending the remote loopback commands described in the next section. A far-end device can also set your device in line loopback by sending standard line loopback set and reset code, or in data port loopback by sending 127 set code and 127 reset code (V.54 loop code).*

## Using the command line

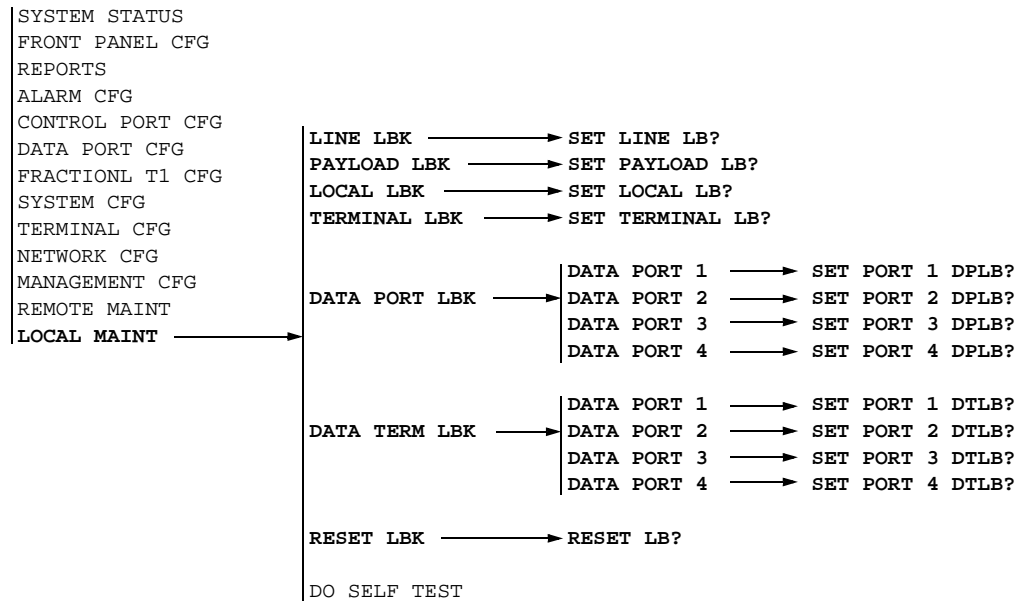
The figure below illustrates the Local Maintenance menu. You use the commands in this menu to set or reset loopbacks in your local device. You must have super-user, configuration, or maintenance privileges.



To reset a loopback in your local DataSMART MAX, enter **RLB**.

## Using the front panel

To set or reset local loopbacks from the front panel, use these steps. You must have super-user, configuration, or maintenance privileges.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until LOCAL MAINT appears in the display.
- 3 Push Select. LINE LBK appears in the display.
- 4 Push Next or Previous until the desired command appears in the display. Note that the RESET LBK command is only available if any loopback has already been set.
- 5 Push Select. If you select either the data port loopback or the data terminal loopback, you must select the desired data port. Push Next or Previous until the desired data port appears in the display and push Select.
- 6 A query asks you if you really want to set or reset the loopback. Push Select to set the loopback. LOOPBACK SET appears in the display.
- 7 After a few seconds, the message RESET LBK appears (“resetting” the loopback turns it off). When you are ready to turn the loopback off, push Select. A query asks if you really want to reset the loopback; push Select to turn off the loopback.

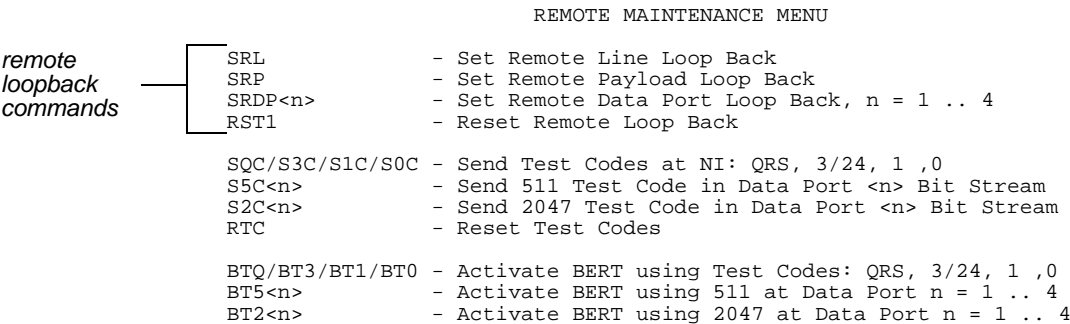
# Setting and resetting loopbacks remotely

You can set a line, payload, or data port loopback remotely, in a far-end device. If you set one of these loopbacks, you can then send test code through the loop and run BERTs on the code to troubleshoot for errors. This section describes how to set and reset remote loopbacks. For a description of how to set and run test codes and BERTs, see page 150.

Only one loopback, either local or remote, may be set at one time. You cannot set a loopback if another loopback is already active, if test code is being transmitted, or if a BERT is active.

## Using the command line

The figure below illustrates the Remote Maintenance menu. You use the commands listed in this menu to set and reset remote loopbacks. You must have super-user, configuration, or maintenance privileges.



- SRL** Set a remote line loopback.
- SRP** Set a remote payload loopback.
- SRDP<sub>n</sub>** Set a remote data port loopback on data port *n*, where *n* is the number of the data port: 1 or 2 in dual-port devices; 1, 2, 3, or 4 in quad-port devices.

To reset a remote loopback, enter **RST1**.

You may receive one or more of the following messages when setting or resetting remote loopbacks.

SENDING LOOP BACK SET CODE — The DataSMART MAX is requesting a loopback.

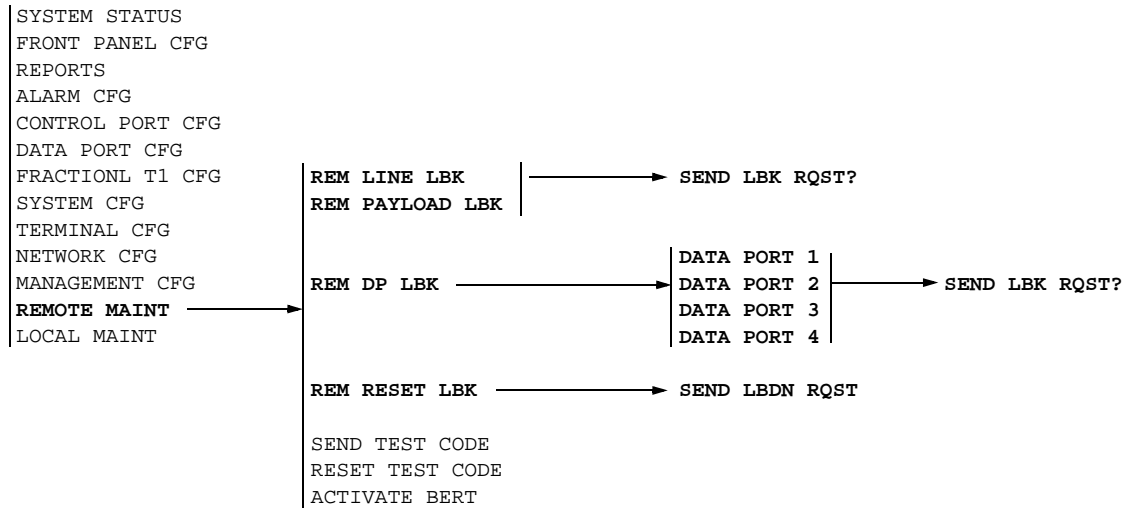
REMOTE LOOP BACK IS SET— The remote loopback is set.

UNABLE TO CONFIRM REMOTE LOOP BACK IS SET — The DataSMART MAX tried to set the remote loopback but was unable to confirm that the loopback was set.

UNABLE TO SET REMOTE LOOP BACK — The DataSMART MAX cannot set a loopback because a loopback is already set, a test code is being generated, or a BERT is active.

## Using the front panel

To set remote loopbacks from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until REMOTE MAINT appears in the display.
- 3 Push Select. REM LINE LBK appears in the display.
- 4 Push Next or Previous until the desired loopback appears in the display.
- 5 Push Select. If you select the remote data port loopback, you must select the desired data port. Push Next or Previous until the desired data port appears in the display, then push Select.
- 6 A query asks if you really want to set the loopback. Push Select to set the loopback. LOOPBACK SET appears in the display.
- 7 If you want to reset a remote loopback (turn the loopback off), push Select when REM RESET LBK appears in the display. You will be asked to verify this selection. Push Select again.

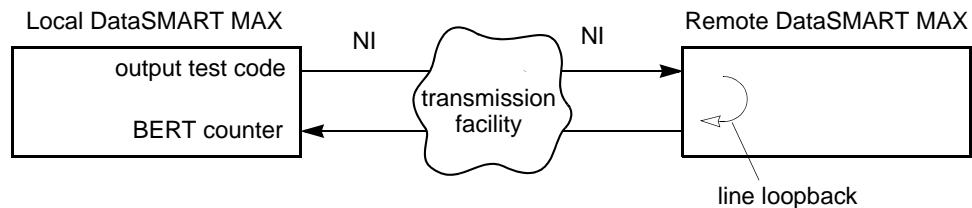
When you send a request to set or reset a loopback, you will receive one of several responses:

SENDING RQST	The DataSMART MAX is in the process of sending the request.
NO CONFIRMATION	The DataSMART MAX sent the request, but was unable to confirm that the loopback was set or reset.
LPBK CONFIRMED	The DataSMART MAX sent the request and the loopback was confirmed as set or reset.
UNABLE TO SEND	The DataSMART MAX is unable to send the request because a loopback is already set, a test code is being sent, or a BERT is active.

---

## Using test codes and BERTs

When you set a remote loopback in a far-end device, you'll usually want to run a bit error rate test (BERT) on the looped signal. A BERT allows you to send a test code through a looped back line, then counts the errors returned in the signal. For example, the figure below illustrates how you might use a BERT in conjunction with a line loopback.



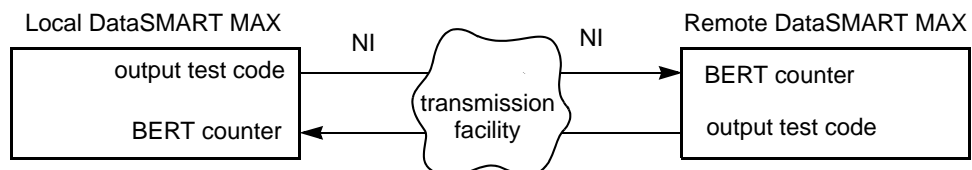
To use a BERT in conjunction with a remote loopback, do the following:

- 1 Set the remote loopback. You can set a remote line or payload loopback to test the full T1 signal, or you can set a data port loopback to test the channels assigned to a specific data port.
- 2 Send test codes through the loop. To test the full T1 signal, send one of the following test codes: QRS, 3 in 24, all 1s, or all 0s.

To test the channels assigned to a specific data port, send one of the following codes on those channels: 511 or 2047.

- 3 Activate the BERT and monitor the BERT error report.
- 4 Exit BERT.
- 5 Reset the test codes.
- 6 Reset the loopback.

You can also use BERT in a bi-directional, point-to-point test. In this application, you set each DataSMART MAX in the point-to-point connection to output specific test code. Then you activate BERT on that test code in each device. This allows you to test the T1 signal between the network interfaces of the two devices.



## How BERTs work

When a BERT is first activated, the DataSMART MAX initializes all counters to zero. It starts monitoring the incoming network signal for the specified test pattern. (In the case of a data port loopback, the DataSMART MAX looks for the specified test pattern only on the channels mapped to the specified data port.)

When the DataSMART MAX recognizes the test pattern, it begins tracking time and errors. The time counter continues to count even during time of sync loss. The time and error counters continue to count until they reach their maximum limit as specified below; they do not roll over.

You can exit BERT by typing Ctrl-C.

```
RM> btq
^C to TERMINATE
SEARCHING FOR PATTERN
Pattern Detected
```

TEST SECONDS	BIT ERRORS	ERRORED SECONDS	BURSTY SECONDS	SEV ERR SECONDS	UNAVAIL SECONDS	TOTAL BIT ERRORS
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	1	1	0	0	0	1
9	3	2	1	0	0	4
10	5	3	2	0	0	9
11	6	4	3	0	0	15
12	5	5	4	0	0	20
13	5	6	5	0	0	25
14	5	7	6	0	0	30
15	4	8	7	0	0	34
16	0	8	7	0	0	34
17	0	8	7	0	0	34
18	0	8	7	0	0	34
19	0	8	7	0	0	34
20	0	8	7	0	0	34

Field	Description
TEST SECONDS	The number of seconds, up to 2 <sup>32</sup> maximum, that the DataSMART MAX has been running the test after first detecting the test pattern.
BIT ERRORS	The number of bit errors, up to 65,535 maximum, that have occurred in the current second.
ERRORED SECONDS	The number of errored seconds, up to 65,535 maximum, that have occurred since the DataSMART MAX first detected the test pattern.
BURSTY SECONDS	The number of bursty errored seconds, up to 65,535 maximum, that have occurred since the DataSMART MAX first detected the test pattern.
SEV ERR SECONDS	The number of severely errored seconds, up to 65,535 maximum, that have occurred since the DataSMART MAX first detected the test pattern.
UNAVAIL SECONDS	The number of unavailable seconds, up to 65,535 maximum, that have occurred since the DataSMART MAX first detected the test pattern.

Field	Description
TOTAL BIT ERRORS	The running total of bit errors, up to $2^{32}$ maximum, that have occurred since the DataSMART MAX first detected the test pattern.

## Command-line access

You set and reset test codes and activate a BERT by using the commands listed in the Remote Maintenance menu. You must have super-user, configuration, or maintenance privileges to use these commands.

REMOTE MAINTENANCE MENU	
	SRL - Set Remote Line Loop Back
	SRP - Set Remote Payload Loop Back
	SRDP<n> - Set Remote Data Port Loop Back, n = 1 .. 4
	RSTl - Reset Remote Loop Back
test code commands	SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1, 0
	S5C<n> - Send 511 Test Code in Data Port <n> Bit Stream
	S2C<n> - Send 2047 Test Code in Data Port <n> Bit Stream
	RTC - Reset Test Codes
BERT commands	BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1, 0
	BT5<n> - Activate BERT using 511 at Data Port n = 1 .. 4
	BT2<n> - Activate BERT using 2047 at Data Port n = 1 .. 4

Each test code is sent out framed. To set and reset test codes:

<b>SQC</b>	Send framed QRS code out the network interface.
<b>S3C</b>	Send framed 3-in-24 code out the network interface.
<b>S1C</b>	Send all 1s out the network interface. This may be required by the carrier.
<b>S0C</b>	Send all 0s out the network interface.
<b>S2Cn</b>	Send 2047 code in the channels assigned to data port <i>n</i> , where <i>n</i> is the number of the data port: 1 or 2 in a dual-port device; 1, 2, 3, or 4 in a quad-port device.
<b>S5Cn</b>	Send 511 code in the channels assigned to data port <i>n</i> , where <i>n</i> is the number of the data port: 1 or 2 in a dual-port device; 1, 2, 3, or 4 in a quad-port device.
<b>RTC</b>	Reset the test code generation.

To activate a BERT on the test codes:

<b>BTQ</b>	Activate a BERT on QRS test code.
<b>BT3</b>	Activate a BERT on 3-in-24 test code.
<b>BT1</b>	Activate a BERT on all 1s test code.
<b>BT0</b>	Activate a BERT on all 0s test code.
<b>BT2n</b>	Activate a BERT on 2047 test code in channels assigned to data port <i>n</i> .
<b>BT5n</b>	Activate a BERT on 511 test code in channels assigned to data port <i>n</i> .

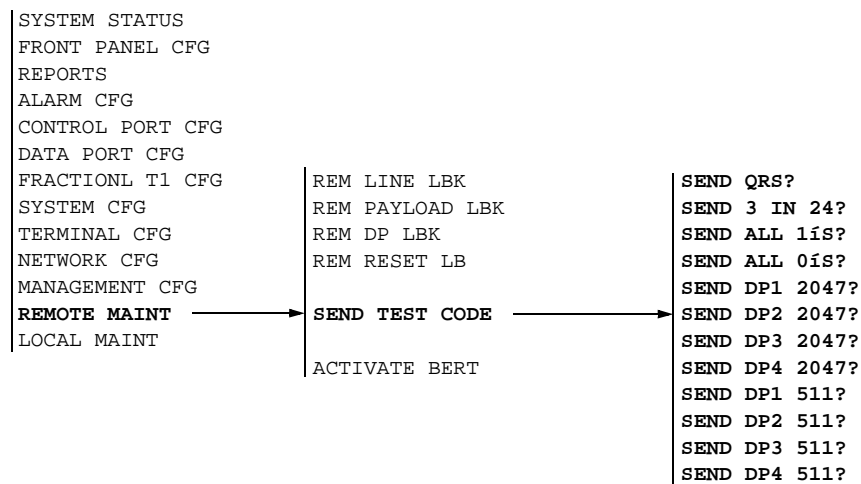
To de-activate or exit a BERT, enter Ctrl-C.



When you first activate a BERT, you will receive the message SEARCHING FOR PATTERN. When the DataSMART MAX recognizes the test pattern, the BERT report will appear on the display.

Front-panel access

To set and reset test codes from the front panel, use these steps.



- 1

Push Escape until SYSTEM STATUS appears in the display.
- 2

Push Next or Previous until REMOTE MAINT appears in the display.
- 3

Push Select. REM LINE LBK appears in the display.
- 4

Push Next or Previous until SEND TEST CODE appears in the display.
- 5

Push Select. SEND QRS? appears in the display.
- 6

Push Next or Previous until the desired test code appears in the display.
- 7

Push Select to send the test code. You may receive one of the following responses:

UNABLE TO SET

This means DataSMART MAX is not able send the test code to the far-end device because another test condition exists.

NO CHAN ASSIGNED

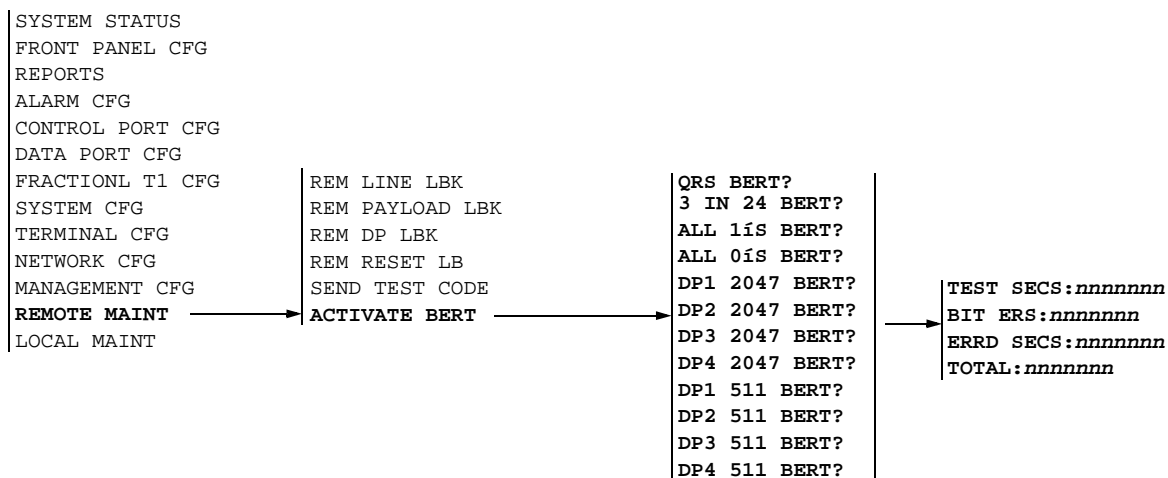
This means DataSMART MAX is not able to send 2047 or 511 test code because the specified data port has no assigned channels.
- 8

After a few seconds, the message RESET TEST CODE appears. Push Select when you want to stop sending test code. You are asked to confirm the selection. You may receive the following response:

UNABLE TO CLEAR

The DataSMART MAX is not able to reset the test code.

To activate a BERT, use the following steps. To deactivate a BERT, push Escape.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until REMOTE MAINT appears in the display.
- 3 Push Select. REM LINE LBK appears in the display.
- 4 Push Next or Previous until ACTIVATE BERT appears in the display.
- 5 Push Select. QRS BERT? appears in the display.
- 6 Push Next or Previous until the desired BERT appears in the display.
- 7 Push Select to activate the BERT. The display will show SEARCHING, indicating that the DataSMART MAX is searching for the specified test code in the incoming signal. When it finds it, the first readout in the list below appears. Push Next or Previous to see the other readouts. The readouts are updated dynamically as long as the BERT is active.

TEST SECS: nnnnnnnn	The number of seconds, up to 65,535 maximum, since the test pattern was first detected.
BIT ERS: nnnnnnnn	The number of bit errors, up to 65,535 maximum, that have occurred in the current second.
ERRD SECS: nnnnnnnn	The number of errored seconds, up to 65,535 maximum, that have occurred since the DataSMART MAX first detected the test pattern.
TOTAL: nnnnnnnn	The total number of bit errors since the test code was first detected.

# 7

## *Using network management*

---

DataSMART MAX supports network management via Telnet and the Simple Network Management Protocol (SNMP).

This chapter tells you:

- How to configure for Telnet
- How to configure for SNMP

---

## Basic network management configuration (Telnet)

To manage DataSMART MAX with SNMP or Telnet, you must configure the unit to operate with TCP/IP networks. The base level of functionality is configuring the unit for management via Telnet.

### Stand-alone units

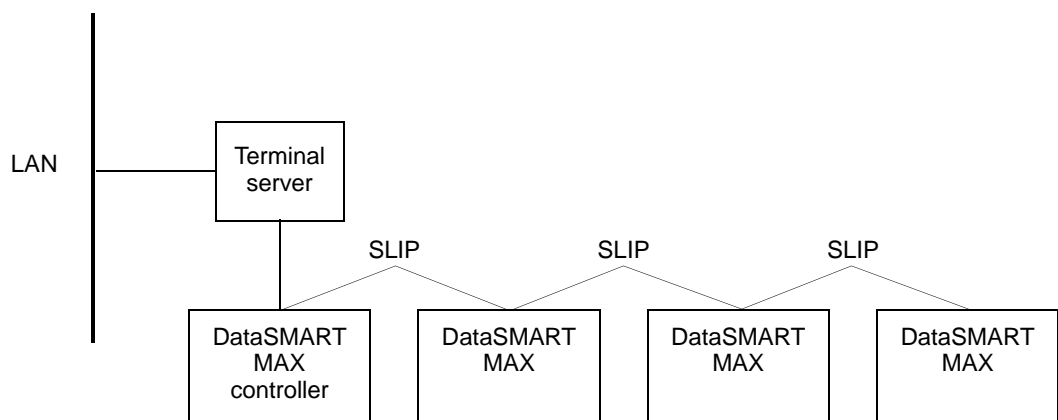
To configure a stand-alone DataSMART MAX unit for management via Telnet, you must:

- Set the IP address and IP netmask of the unit.
- Set the default router address of the unit. The default router must be on the same subnet as the DataSMART MAX.
- Set the Telnet password.
- Set up IP address screening, if extra IP network security is desired.
- Select the IP network interface. This can be SLIP or Ethernet (not both simultaneously).

### Daisy-chained units, using SLIP

To configure daisy-chained units for Telnet access via SLIP, you must:

- Set the IP address and IP netmask of each unit's SLIP interface. These addresses must all be on the same subnet.
- Set the default router address for the units. The default router address is typically the SLIP IP address of the terminal server; it must be on the same subnet as the SLIP IP addresses of the units. All units must be set to the same default router.
- Set the Telnet password for each unit.
- Set up IP address screening, if extra IP network security is desired.
- Set the IP network interface of each unit to SLIP.

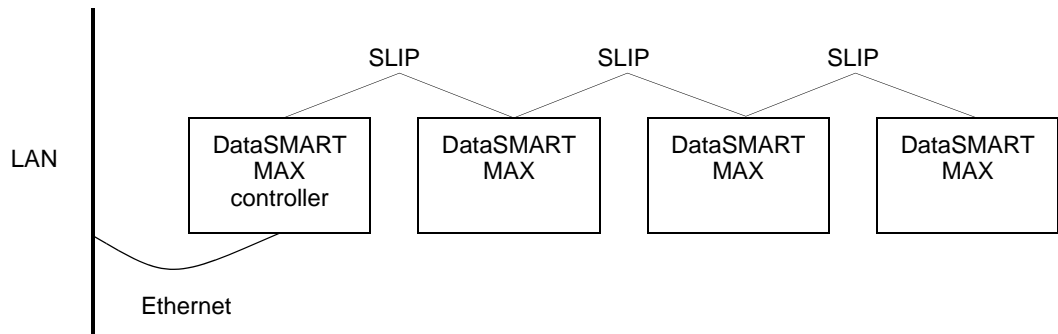


The IP addresses and netmasks of all units in the chain, including the controller, must be on the same subnet.

## Daisy-chained units, using Ethernet

To configure daisy-chained units for Telnet access via Ethernet, you must:

- Set up an IP address and netmask for both the SLIP interface and the Ethernet interface on the controller unit. The SLIP and Ethernet IP addresses must be on separate subnets; the interfaces can share the same netmask.
- Set the IP address and IP netmask of each chained unit's SLIP interface. These addresses must all be on the same subnet as each other and as the controller unit's SLIP interface.
- Set the default router address for each unit. The default router address for the controller must be on the same subnet as the controller's Ethernet address. The default router address for the chained units must be the SLIP IP address of the controller, since the controller is the default router for the chained units.
- Set the Telnet password for each unit.
- Set up IP address screening, if extra IP network security is desired.
- Set the IP network interface of the controller unit to Both, and set the interface for each chained unit to SLIP.



The SLIP IP addresses of all units in the chain, including the controller, must be on the same subnet. The Ethernet address of the controller must be on a separate subnet.

Command-line  
access

Enter MC to display the Management Configuration menu.

MANAGEMENT CONFIGURATION MENU	
ESNMP/DSNMP	- Enable/Disable SNMP Agent
TCS:<str>	- Set SNMP Trap Comm String, str=1 to 15 characters
RCS:<str>	- Set SNMP Read Comm String, str=1 to 15 characters
WCS:<str>	- Set SNMP Write Comm String, str=1 to 15 characters
TPW:<str>	- Set Telnet Password, str=0 to 15 characters 0 characters disables Telnet
SSA:<c>	- Set Packet Screening via Source Address c = (IP Addr), N (None)
NETIF:<c>	- Set IP Network Interface c = N (None), S (SLIP), E (Ethernet), B (Both)
IPR:<ipa>	- Set DSU Default Route IP Address
IPA:<c><ipa>	- Set DSU IP Addresses
IPM:<c><mask>	- Set DSU IP Mask c = S (SLIP), E (Ethernet)
ADD:<list>,<ipa>	- Add Address to Screening or Trap Dest Lists
DEL:<list>,<ipa>	- Delete Address to Screening or Trap Dest Lists <list> = I (IP Addr), T (Trap) <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
MCV	- View Management Configuration

Front-panel access

Front-panel access is provided through the MANAGEMENT CFG menu.

SYSTEM STATUS	
FRONT PANEL CFG	SNMP AGENT —————> ENABLE DISABLE
REPORTS	TRAP COM STRING —————> xxxxxxxxxxxxxxxx
ALARM CFG	READ COM STRING —————> xxxxxxxxxxxxxxxx
CONTROL PORT CFG	WRITE COM STRING —————> xxxxxxxxxxxxxxxx
DATA PORT CFG	TELNET PASSWORD —————> xxxxxxxxxxxxxxxx
FRACTIONL T1 CFG	SRC ADDR SCREEN —————> IP_ADDR NONE
SYSTEM CFG	IP NETWORK INTF —————> NONE SLP ETH BOTH
TERMINAL CFG	DSU DEFLT ROUTE —————> nnn.nnn.nnn.nnn
NETWORK CFG	SLIP IP ADDRESS —————> nnn.nnn.nnn.nnn
MANAGEMENT CFG —————>	SLIP IP MASK —————> nnn.nnn.nnn.nnn
REMOTE MAINT	ETHER IP ADDRESS —————> nnn.nnn.nnn.nnn
LOCAL MAINT	ETHER IP MASK —————> nnn.nnn.nnn.nnn
	ADD TRAP ADDR —————> nnn.nnn.nnn.nnn
	ADD SCREEN ADDR —————> nnn.nnn.nnn.nnn
	DEL/VW TRAP ADDR —————> nnn.nnn.nnn.nnn
	DEL/VW SCRN ADDR —————> nnn.nnn.nnn.nnn

## View the current settings

Before changing any management parameters, you may want to look at the current settings. You do this by executing the **MCV** command. This command displays the View Management Configuration screen. To see the Telnet password, you must have super-user privileges.

```

VIEW MANAGEMENT CONFIGURATION

SNMP Agent   Trap Comm String   Read Comm String   Write Comm String
-----
DISABLED     snmptrap           public             private

Telnet Password   Addr Screening   IP Net Interfaces   IP Default Router
-----
                NONE             NONE                192.0.2.2

SLIP IP Addr     SLIP IP Mask      Ethernet IP Addr     Ethernet IP Mask
-----
192.0.2.1        255.255.255.0     192.0.2.2           255.255.255.0

IP Addr Screening   Trap Dest IP Addr
-----

```

Field	Description
SNMP Agent	This field tells you if the SNMP Agent is enabled or disabled.
Trap Comm String	This field tells you the current value of the SNMP Trap Community String. The default value is “snmptrap”.
Read Comm String	This field tells you the current value of the SNMP Read Community String. The default value is “public”.
Write Comm String	This field tells you the current value of the SNMP Write Community String. The default value is “private”.
Telnet Password	This field tells you the current Telnet password. If there is no Telnet password, the Telnet Server will not be active and you will not be able to Telnet to the unit.
Addr Screening	This field tells you if IP addresses are currently being screened by the unit.
IP Net Interfaces	This field tells you if the IP network interface is enabled. If it is enabled, it indicates whether the unit is using the Ethernet interface, the SLIP interface, or both (i.e., the unit is configured as a daisy-chained controller).
IP Default Router	This field tells you the address of the IP Router the unit must send packets to in order to get them into the IP network.
SLIP IP Addr	This field shows the SLIP IP address the unit is currently using.
SLIP IP Mask	This field shows the SLIP IP netmask the unit is currently using.
Ethernet IP Address	This field shows the Ethernet IP address the unit is currently using.
Ethernet IP Mask	This field shows the Ethernet IP netmask the unit is currently using.
IP Addr Screening	This field shows which IP addresses are allowed to communicate with the unit. This field can have up to ten entries. Duplicate entries are not valid.

## Setting the IP addresses and netmasks

Field	Description
Trap Dest IP Addr	This field tells you which IP addresses the unit sends traps to. This field can have up to ten entries. Duplicate entries are valid.

Every device (or host) on an IP network requires a unique IP address and an IP netmask. IP addresses and netmasks are 32-bit bitmaps, but DataSMART MAX uses the industry short-hand convention of four numbers with ranges from 0 to 255. This shorthand looks like *aaa.bbb.ccc.ddd*. If you do not know the numbers for your IP addresses and IP netmasks, ask your system administrator.

### IP addresses

The IP address is the unique address for a unit in the IP network. When you assign the IP address, you need to specify whether the address is for the unit's SLIP or Ethernet interface.

Stand-alone units can use only one interface at a time, either SLIP or Ethernet. For instructions on enabling the interface, see [“Selecting the IP network interface” on page 171](#).

If you have configured a daisy-chain and are accessing the controller unit via Ethernet, you need to assign the controller unit an Ethernet IP address (for receiving packets) and a SLIP IP address (for packet output to the rest of the chain). The Ethernet and SLIP IP addresses must be on different subnets. The other units in the chain must be assigned SLIP IP addresses on the same subnet as the controller unit's SLIP IP address.

The default SLIP IP address is 192.0.2.1. The default Ethernet IP address is also 192.0.2.1.

### Using the command line

You set the IP addresses by using the **IPA** command. You must have super-user or configuration privileges. The changed IP address takes effect only after you have logged out.

The command syntax is:

**IPA:***c,ipa*

*c*                      **S** assigns the IP address to the SLIP interface.  
                         **E** assigns the IP address to the Ethernet interface.

*ipa*                    Specifies the IP address as:  
                         *nnn.nnn.nnn.nnn*    where *nnn* = 0 ... 255, but 0.0.0.0 is not valid.

### Using the front panel

The changed IP address takes effect immediately upon pushing Select. To set the SLIP IP



address or Ethernet IP address from the front panel, use these steps.

SYSTEM STATUS		
FRONT PANEL CFG		
REPORTS		
ALARM CFG		
CONTROL PORT CFG		
DATA PORT CFG		
FRACTIONL T1 CFG		
SYSTEM CFG		
TERMINAL CFG		
NETWORK CFG		
MANAGEMENT CFG	→	
REMOTE MAINT		
LOCAL MAINT		
		SNMP AGENT
		TRAP COM STRING
		READ COM STRING
		WRITE COM STRING
		TELNET PASSWORD
		SRC ADDR SCREEN
		IP NETWORK INTF
		DSU DEFLT ROUTE
		SLIP IP ADDRESS → <i>nnn.nnn.nnn.nnn</i>
		SLIP IP MASK
		ETHER IP ADDRESS → <i>nnn.nnn.nnn.nnn</i>
		ETHER IP MASK
		ADD TRAP ADDR
		ADD SCREEN ADDR
		DEL/VW TRAP ADDR
		DEL/VW SCRNR ADDR

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Next or Previous until SLIP IP ADDRESS or ETHER IP ADDRESS, depending upon which address you want to define, appears in the display.
- 5 Push Select. The current IP address appears in the display.
- 6 Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.
- 7 Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
- 8 If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP address or push Escape to abort.

## IP netmask

DataSMART MAX uses the IP netmask to determine if a packet is destined for a unit on the same IP network as itself. If the packet is destined for its network, DataSMART MAX can send the packet directly to the host. If the packet is destined for a different network, DataSMART MAX must send the packet to the IP address of its default router. The default router must be on the same IP network as DataSMART MAX. If there is no default router defined, or if the definition is invalid, DataSMART MAX discards the packet.

If the DataSMART MAX is being configured as a controller in a daisy-chain, you can assign a different IP netmask to the SLIP interface and Ethernet interface. However, if your system administrator prefers, both interfaces can share the same IP netmask.

The default SLIP IP netmask is 255.255.255.0. The default Ethernet IP netmask is also 255.255.255.0. Changes to the IP netmask take effect upon logout.

## Using the command line

You set the IP netmask by using the **IPM** command. You must have super-user or configuration privileges. The command syntax is:

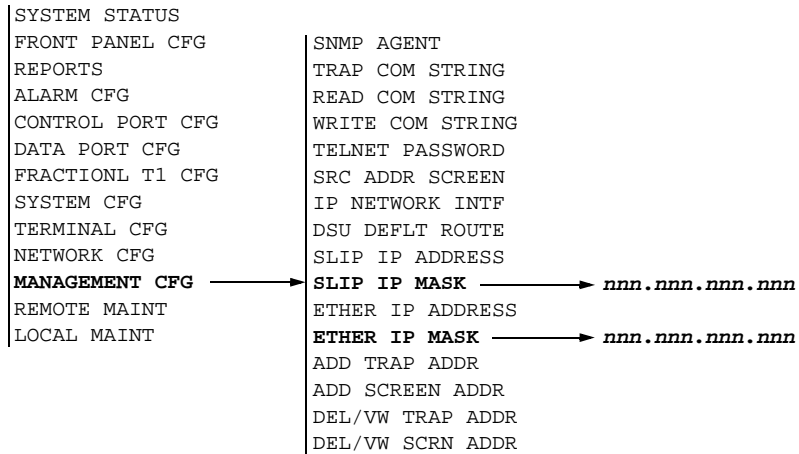
**IPM:***c,mask*

*c*                      **S** assigns the IP address to the SLIP interface.  
                         **E** assigns the IP address to the Ethernet interface.

*mask*                      Specifies the IP address as:  
                         *nnn.nnn.nnn.nnn*    where *nnn* = 0 ... 255, but 0.0.0.0 is not valid.

## Using the front panel

To set the IP netmasks from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Next or Previous until SLIP IP MASK or ETHER IP MASK, depending upon which address you want to define, appears in the display.
- 5 Push Select. The current IP netmask appears in the display.
- 6 Push Next or Previous to move between the four fields of the IP netmask. When the field you want has its first character underlined, push Select.
- 7 Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
- 8 If the entire IP netmask is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP netmask or push Escape to abort.

# Setting the default router IP address

Hosts that are on the same IP network can send packets to each other directly. If the DataSMART MAX needs to send packets to a host that is not on the same network, the packets must be sent to a router that understands the topography of the network. DataSMART MAX needs to know the address of its default router in order to send packets to another network. This could occur if an SNMP management station is on a different network and is trying to retrieve information from a DataSMART MAX.

If the DataSMART MAX unit is a stand-alone, the default router IP address must be on the same IP subnet as the unit's enabled interface (i.e., SLIP or Ethernet).

If the DataSMART MAX unit is a controller in a daisy-chain and is configured for Ethernet access, the default router address must be on the same subnet as the unit's Ethernet IP address. If the controller unit is configured for SLIP, the default router address must be on the same subnet as the unit's SLIP IP address. The default router address for the other units in the chain must be the SLIP IP address of the controller unit.



## NOTE

*You should always set the address of the default router. If a default router does not exist and DataSMART MAX tries to send a packet to a host not on its subnet, the packet will be discarded. This is true for Ethernet and SLIP connections.*

The default value is 192.0.2.2.

## Using the command line

You set the default router by using the **IPR** command. The syntax for the command is shown below. You must have super-user or configuration privileges.

**IPR:***ipa*

The *ipa* value specifies the IP default router as:

*nnn.nnn.nnn.nnn* where *nnn* = 0 ... 255, but 0.0.0.0 is not valid.

## Using the front panel

To set the IP address of the default router from the front panel, use these steps.

SYSTEM STATUS	
FRONT PANEL CFG	SNMP AGENT
REPORTS	TRAP COM STRING
ALARM CFG	READ COM STRING
CONTROL PORT CFG	WRITE COM STRING
DATA PORT CFG	TELNET PASSWORD
FRACTIONL T1 CFG	SRC ADDR SCREEN
SYSTEM CFG	IP NETWORK INTF
TERMINAL CFG	<b>DSU DEFLT ROUTE</b> → <i>nnn . nnn . nnn . nnn</i>
NETWORK CFG	SLIP IP ADDRESS
<b>MANAGEMENT CFG</b> →	SLIP IP MASK
REMOTE MAINT	ETHER IP ADDRESS
LOCAL MAINT	ETHER IP MASK
	ADD TRAP ADDR
	ADD SCREEN ADDR
	DEL/VW TRAP ADDR
	DEL/VW SCRN ADDR

- 1** Push Escape until SYSTEM STATUS appears in the display.
- 2** Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3** Push Select. SNMP AGENT appears in the display.
- 4** Push Next or Previous until DSU DEFLT ROUTE appears in the display.
- 5** Push Select. The IP address of the current default router appears in the display.
- 6** Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.
- 7** Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
- 8** If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP address or push Escape to abort.

## Setting the Telnet password

The DataSMART MAX Telnet server is enabled and disabled via the Telnet password. A null password (i.e. "", string length of zero) disables Telnet. Any non-null string enables Telnet. The Telnet password can be up to 15 characters long.

To access the unit via Telnet, the Telnet password must be a non-null string and the IP network interface must be enabled and configured properly.

### Using the command line

You set the Telnet password using the **TPW** command. The syntax for the command is shown below. You must have super-user privileges.

**TPW:***str*

*str* Enter the Telnet password. The password can be up to 15 characters long including spaces (trailing spaces are not truncated).

### Using the front panel

The operation of the front panel for this command is different than most other commands. The display is not dynamic. The Telnet password will not be changed until the very end when you confirm the change. In addition, if someone on the control port changes the Telnet password, the change will not be reflected on the front panel.

Spaces are allowed at the beginning and in the middle of the password. When using the command line, spaces can only be entered in the middle of the password.

To set the Telnet password from the front panel, use these steps.

SYSTEM STATUS	
FRONT PANEL CFG	SNMP AGENT
REPORTS	TRAP COM STRING
ALARM CFG	READ COM STRING
CONTROL PORT CFG	WRITE COM STRING
DATA PORT CFG	<b>TELNET PASSWORD</b> → xxxxxxxxxxxxxxxx
FRACTIONL T1 CFG	SRC ADDR SCREEN
SYSTEM CFG	IP NETWORK INTF
TERMINAL CFG	DSU DEFLT ROUTE
NETWORK CFG	SLIP IP ADDRESS
<b>MANAGEMENT CFG</b> →	SLIP IP MASK
REMOTE MAINT	ETHER IP ADDRESS
LOCAL MAINT	ETHER IP MASK
	ADD TRAP ADDR
	ADD SCREEN ADDR
	DEL/VW TRAP ADDR
	DEL/VW SCRNR ADDR

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Next or Previous until TELNET PASSWORD appears in the display.
- 5 Push Select. The current Telnet password appears in the display.
- 6 Push Next or Previous to move between the fifteen possible characters of the Telnet password. When the character you want is underlined, push Select.
- 7 Push Next or Previous to increment or decrement the value. When the value of the

character field is what you want, push Select.

- 8 If the entire Telnet password is correct, push Escape. You will be prompted with: “SET NEW STRING?”. Push Select to set the IP address or push Escape to abort.

## Setting up IP source address screening

The DataSMART MAX can screen IP packets based on the source IP address. This security feature lets you screen out packets from any host that is not supposed to access the DataSMART MAX.

For instance, if you know that only network managers should access the DataSMART MAX, you can add their host addresses to the IP screening list and lock out all other hosts by adding the host addresses of the network managers to the IP screening list and then enabling IP source address screening.

If the DataSMART MAX is a controller in a daisy-chain and is configured for Ethernet access, the unit screens packets received at its Ethernet interface before forwarding them to its SLIP interface and other units in the chain.

## Adding an address to the IP screening list

Before you can enable IP screening, you must have at least one IP address in the screening list. You can have up to ten addresses total. This list cannot contain multiple entries of the same address, unlike the SNMP trap host list. This list is empty at first power-up.

### Using the command line

You add an IP address to the IP screening list by using the **ADD** command. You must have super-user or configuration privileges. The command syntax is:

**ADD:***list,ipa*

*list*

Enter **I** to indicate you are working with IP source address screening. Entering **T** indicates you are working with trap hosts (for more information, refer to [“Adding an address to the SNMP trap host list” on page 176](#)).

*ipa*

Add the specified IP address to the list. See [“Setting the IP addresses and netmasks” on page 160](#) for a detailed description of the *ipa* field.

### Using the front panel

To add an IP address to the IP screening list from the front panel, use these steps.

SYSTEM STATUS		
FRONT PANEL CFG		SNMP AGENT
REPORTS		TRAP COM STRING
ALARM CFG		READ COM STRING
CONTROL PORT CFG		WRITE COM STRING
DATA PORT CFG		TELNET PASSWORD
FRACTIONL T1 CFG		SRC ADDR SCREEN
SYSTEM CFG		IP NETWORK INTF
TERMINAL CFG		DSU DEFLT ROUTE
NETWORK CFG		SLIP IP ADDRESS
<b>MANAGEMENT CFG</b>	→	SLIP IP MASK
REMOTE MAINT		ETHER IP ADDRESS
LOCAL MAINT		ETHER IP MASK
		ADD TRAP ADDR
		<b>ADD SCREEN ADDR</b> → <i>nnn.nnn.nnn.nnn</i>
		DEL/VW TRAP ADDR
		DEL/VW SCRN ADDR

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Next or Previous until ADD SCREEN ADDR appears in the display.
- 5 Push Select. The IP address of the first host in the list appears in the display.
- 6 Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.
- 7 Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
- 8 If the entire IP address is correct, push Escape. You will be prompted with: “SET NEW ADDRESS?”. Push Select to set the IP address or push Escape to abort.

## Deleting an address from the IP screening list

To delete an address from the IP screening list, source address screening must be disabled. Enabling or disabling source address screening does not take effect until you log out and log back in.

### Using the command line

You delete an address from the IP screening list by using the **DEL** command. You must have super-user or configuration privileges. The command syntax is:

**DEL:***list,ipa*

*list*

Enter **I** to indicate you are working with IP source address screening. Entering **T** indicates you are working with trap hosts (for more information, refer to [“Adding an address to the SNMP trap host list” on page 176](#)).

*ipa*

Delete the specified SNMP manager’s IP address from the list. See [“Setting the IP addresses and netmasks” on page 160](#) for a detailed description of the *ipa* field.

or

**DEL:****I:**\*

Delete all entries in the list by using the \* wildcard.



## Using the front panel

To remove an IP address from the IP screening list from the front panel, use these steps.

SYSTEM STATUS	
FRONT PANEL CFG	
REPORTS	
ALARM CFG	
CONTROL PORT CFG	
DATA PORT CFG	
FRACTIONL T1 CFG	
SYSTEM CFG	
TERMINAL CFG	
NETWORK CFG	
<b>MANAGEMENT CFG</b> →	SNMP AGENT
REMOTE MAINT	TRAP COM STRING
LOCAL MAINT	READ COM STRING
	WRITE COM STRING
	TELNET PASSWORD
	SRC ADDR SCREEN
	IP NETWORK INTF
	DSU DEFLT ROUTE
	SLIP IP ADDRESS
	SLIP IP MASK
	ETHER IP ADDRESS
	ETHER IP MASK
	ADD TRAP ADDR
	ADD SCREEN ADDR
	DEL/VW TRAP ADDR
	DEL/VW SCRN ADDR → <i>nnn.nnn.nnn.nnn</i>

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Next or Previous until DEL/VW SCRN ADDR appears in the display.
- 5 Push Select. The IP address of the first host in the list appears in the display.
- 6 Push Next or Previous to move through the screening list. When you find the IP address you wish to delete, push Select.
- 7 Continue deleting addresses, or push Escape to return to the DEL/VW SCRN ADDR level.

Enabling and disabling IP source address screening

You can enable IP source address screening after filling in the IP addresses allowed access to the DataSMART MAX.

The default is address screening disabled.

Using the command line

You set the IP Source Address Screening using the **SSA** command. You must have super-user or configuration privileges. The command syntax is:

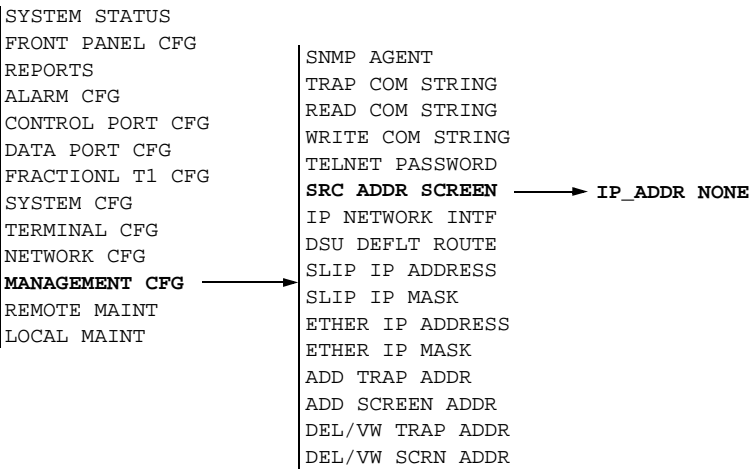
**SSA:***c*

The *c* parameter specifies the address screening.

- I** Screen based on IP source addresses.
- N** No IP address screening.

Using the front panel

To enable or disable IP source address screening from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select, then push Next until SRC ADDR SCREEN appears in the display.
- 4 Push Select. The current state of IP screening appears in the display.
- 5 Push Next or Previous to move between IP\_ADDR and NONE. When the value you want is displayed, push Select.

## Selecting the IP network interface

The DataSMART MAX can access IP networks via Ethernet protocol or SLIP.

To use the Ethernet interface, the Ethernet card must be inserted in the PCMCIA card slot on the rear of the unit.

To use SLIP, you must connect to a router, terminal server, or computer with a SLIP interface. When the unit is configured for SLIP, only IP packets are recognized on the control ports. Daisy-chained units still work as long as each unit in the chain is configured for SLIP and has its own unique IP address on the same IP network. The **DCE/DTE** command determines which port processes IP packets. All packets received are transmitted out the other port.

If the DataSMART MAX is a stand-alone unit, it should be set to either Ethernet (**E**) or SLIP (**S**), but not both. Only one interface can be active at any one time.

If the DataSMART MAX is a controller in a daisy-chain and is configured for Ethernet access, the unit should be set to use both (**B**) interfaces. If the unit is configured for SLIP access, it should be set to SLIP (**S**). The other units in the chain should always be set to SLIP (**S**).



### NOTE

*Your system administrator may have to establish IP routing tables on the Ethernet LAN to support the daisy-chain controller feature.*

DataSMART MAX is a single Telnet device. If a Telnet session is active and the IP network fails, the Telnet session is still active. For this reason, auto-logout is always enabled when Telnet is being used. If auto-logout was disabled before a Telnet session is started, auto-logout is set to 15 minutes for that Telnet session. When the user logs out, auto-logout reverts to the default configuration value. If auto-logout is enabled before a Telnet session is started, auto-logout will not be changed.

### Using the command line

You set the network interface by using the **NETIF** command. You must have super-user or configuration privileges. Changes to the IP network interface take effect upon logout. When shipped from the factory, the network interface is set to none. The command syntax is:

**NETIF:***c*

The *c* parameter specifies the network interface as:

<b>N</b>	None
<b>S</b>	SLIP interface
<b>E</b>	Ethernet interface
<b>B</b>	Both SLIP and Ethernet interfaces

## Using the front panel

To set the IP network interface from the front panel, use these steps.

SYSTEM STATUS	
FRONT PANEL CFG	
REPORTS	
ALARM CFG	
CONTROL PORT CFG	
DATA PORT CFG	
FRACTIONL T1 CFG	
SYSTEM CFG	
TERMINAL CFG	
NETWORK CFG	
<b>MANAGEMENT CFG</b> →	
REMOTE MAINT	
LOCAL MAINT	

SNMP AGENT	
TRAP COM STRING	
READ COM STRING	
WRITE COM STRING	
TELNET PASSWORD	
SRC ADDR SCREEN	
<b>IP NETWORK INTF</b> →	<b>NON SLP ETH BTH</b>
DSU DEFLT ROUTE	
SLIP IP ADDRESS	
SLIP IP MASK	
ETHER IP ADDRESS	
ETHER IP MASK	
ADD TRAP ADDR	
ADD SCREEN ADDR	
DEL/VW TRAP ADDR	
DEL/VW SCRNR ADDR	

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display, then push Select. Push Next until IP NETWORK INTF appears in the display.
- 3 Push Select to enter the IP NETWORK INTF command. The current IP network interface setting appears in the display.
- 4 Push Next or Previous to move between NON, SLP, ETH, and BTH. When the value you want is displayed, push Select.

---

# Configuring for SNMP

To enable the SNMP management capabilities of DataSMART MAX, the following parameters must be set:

- Enable the SNMP Agent, SNMP traps, and alarm messages
- Set the SNMP community strings, if necessary
- Add the management hosts to the trap list



## NOTE

*This section assumes you have already set up DataSMART MAX for an IP network. This includes: setting the IP address and netmask, setting the default router, and selecting the network interface.*

## Enabling and disabling the SNMP agent

The DataSMART MAX has a fully functional internal SNMP agent. This agent supports MIB II and the DS1 MIB (RFC 1406), an Enterprise MIB, link up/down, cold-start and warm-start traps.

### Using the command line

You enable and disable the SNMP agent by using the **ESNMP** and **DSNMP** commands, respectively. You must have super-user or configuration privileges.

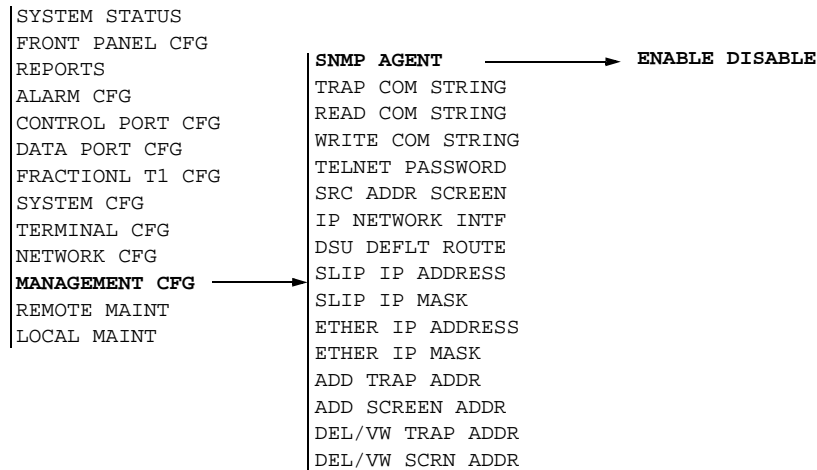
Every time you enable the agent, a warm-start trap is sent from a disabled setting. A cold-start trap is sent after power-up.

The agent is disabled by default.

<b>ESNMP</b>	Enable the SNMP agent.
<b>DSNMP</b>	Disable the SNMP agent.

## Using the front panel

To enable or disable the SNMP agent from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Select. The current state of the SNMP agent appears in the display.
- 5 Push Next or Previous to move between ENABLE and DISABLE. When the value you want is displayed, push Select.

## Setting SNMP community strings

There are three SNMP community strings: read, write, and trap. The community strings are another form of (loose) security. If you want to prevent just any manager from retrieving data from the SNMP agent, you can change the read community string. Make sure that the managers you wish to have access have the same community strings as the ones on DataSMART MAX.

### Read community string

The read community string controls who can read data from the agent. The default value is “public”.

### Write community string

The write community string controls who can write data to the agent using SNMP Sets. The default value is “private”.

### Trap community string

The trap community string controls who can read a trap sent from the agent. The default value is “snmptrap”.

## Using the command line

You set the SNMP community strings by using the **RCS**, **WCS**, and **TCS** commands. You must have super-user or configuration privileges. The command syntax is shown below. The strings are allowed to have spaces in them, but you probably won't want any, as other management stations may not allow spaces in community strings.

**RCS:***str*

**WCS:***str*

**TCS:***str*

where *str* is 1 to 15 characters. Be careful when you enter a string value, trailing spaces are not truncated.

## Using the front panel

The operation of the front panel for these commands is different than most other commands. The display is not dynamic. The community string will not be changed until the very end when you confirm the change. In addition, if someone on the control port changes the community string, the change will not be reflected on the front panel.

To set an SNMP community string from the front panel, use these steps.

SYSTEM STATUS		
FRONT PANEL CFG		
REPORTS		
ALARM CFG		
CONTROL PORT CFG		
DATA PORT CFG		
FRACTIONL T1 CFG		
SYSTEM CFG		
TERMINAL CFG		
NETWORK CFG		
<b>MANAGEMENT CFG</b>	→	SNMP AGENT
REMOTE MAINT		<b>TRAP COM STRING</b> → xxxxxxxxxxxxxxxx
LOCAL MAINT		<b>READ COM STRING</b> → xxxxxxxxxxxxxxxx
		<b>WRITE COM STRING</b> → xxxxxxxxxxxxxxxx
		TELNET PASSWORD
		SRC ADDR SCREEN
		IP NETWORK INTF
		DSU DEFLT ROUTE
		SLIP IP ADDRESS
		SLIP IP MASK
		ETHER IP ADDRESS
		ETHER IP MASK
		ADD TRAP ADDR
		ADD SCREEN ADDR
		DEL/VW TRAP ADDR
		DEL/VW SCRNR ADDR

- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. SNMP AGENT appears in the display.
- 4 Push Next or Previous until TRAP COM STRING appears in the display. If you want to change the trap community string, continue with step 5. Otherwise, continue pushing Next or Previous until you display READ COM STRING or WRITE COM STRING, whichever you want to change.
- 5 Push Select. The current SNMP community string appears in the display.
- 6 Push Next or Previous to move between the fifteen possible characters of the community string. When the character you want is underlined, push Select.
- 7 Push Next or Previous to increment or decrement the value. When the value is what you want, push Select.

- 8 If the entire Telnet password is correct, push Escape. You will be prompted with: “SET NEW STRING?”. Push Select to set the Telnet password or push Escape to abort.

## Configuring the SNMP trap hosts

DataSMART MAX can send SNMP traps to multiple IP network hosts. In order to send SNMP traps, the DataSMART MAX alarm output format must be set to SNMP (see “[Formatting the alarm messages \(ASCII or SNMP\)](#)” on page 62), at least one type of trap must be enabled, the IP Network interface must be set correctly (see “[Selecting the IP network interface](#)” on page 171) and there must be at least one destination in the SNMP trap list. There can be multiple entries of a single address in the SNMP trap list.

## Adding an address to the SNMP trap host list

The SNMP trap host list can have up to ten addresses total. This list is empty at first power-up.

### Using the command line

You add an IP address to the SNMP trap list by using the **ADD** command. You must have super-user or configuration privileges. The command syntax is:

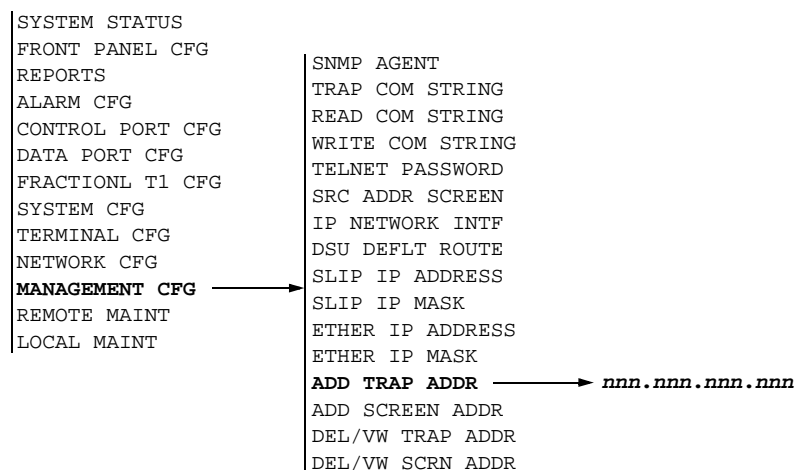
**ADD:list:ipa**

*list* Enter **T** to indicate you are working with the trap host list. Entering **I** indicates you are working with the IP screening list (for more information, refer to “[Adding an address to the IP screening list](#)” on page 166).

*ipa* Add the specified IP address to the list. See “[Setting the IP addresses and netmasks](#)” on page 160 for a detailed description of the *ipa* field.

### Using the front panel

To add an IP address to the SNMP trap list from the front panel, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.
- 3 Push Select. Push Next or Previous until ADD TRAP ADDR appears in the display.



- 4 Push Select. An IP address of 0.0.0.0 appears.
- 5 Push Next or Previous to move between the four groups of the IP address. When the group you want has its first character underlined, push Select.
- 6 Push Next or Previous to increment or decrement the value. When the value is what you want, push Select.
- 7 A question mark appears at the end of the IP address. You will be prompted with: “SET NEW ADDRESS?”. Push Select to set the IP address or push Escape to abort.

## Deleting an address from the SNMP trap list

If there are multiple entries of a single address in the table, each entry must be deleted. One deletion does not clear out all occurrences of that address.

### Using the command line

You delete an address from the SNMP trap list by using the **DEL** command. The syntax for the command is shown below. You must have super-user or configuration privileges.

**DEL:***list:ipa*

*list*

Enter **T** to indicate you are working with the trap host list. Entering **I** indicates you are working with the IP screening list (for more information, refer to [“Adding an address to the IP screening list” on page 166](#)).

*ipa*

Delete the specified SNMP manager’s IP address from the list. See [“Setting the IP addresses and netmasks” on page 160](#) for a detailed description of the *ipa* field.

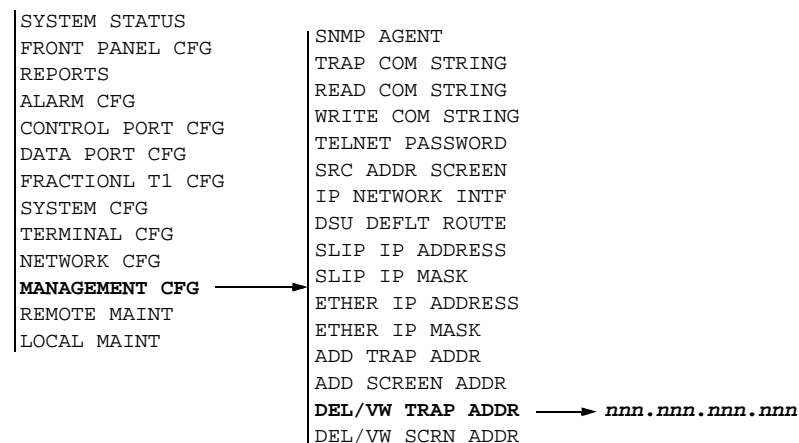
or

**DEL:****T:**\*

Delete all entries in the list by using the \* wildcard character.

### Using the front panel

To delete an IP address from the SNMP trap list, use these steps.



- 1 Push Escape until SYSTEM STATUS appears in the display.
- 2 Push Next or Previous until MANAGEMENT CFG appears in the display.

- 3** Push Select. Push Next or Previous until DEL/VW TRAP ADDR appears in the display.
- 4** Push Select. The IP address of the first host in the list appears in the display.
- 5** Push Next or Previous to move through the screening list. When you find the IP address you wish to delete, push Select.
- 6** Continue deleting addresses, or push Escape to return to the DEL/VW TRAP ADDR level.

---

## Using SNMP traps

SNMP traps are like DataSMART MAX alarm messages: they indicate alarm conditions in the network.

### Configuration for SNMP traps

To use SNMP traps, you must:

- Connect the DataSMART MAX to a TCP/IP network through an Ethernet adapter card installed in the PCMCIA connector, or the SLIP line out the control port.
- Enable the DataSMART MAX SNMP agent by using the **ESNMP** command (see page 173).
- Enable alarm messages in SNMP format by using the **EAM** and **ESM** commands (see pages 61 and 62).

SNMP traps also need a destination IP address. You have ten possible trap destinations defined by the trap host list (see “Configuring for SNMP” on page 173). At the trap host destination there must be an SNMP network management application, such as SunNet Manager, or HP OpenView. These programs understand SNMP and can interact intelligently with the DataSMART MAX SNMP agent.

### Possible types of SNMP traps

DataSMART MAX can generate these trap types:

- Warm-start
- Cold-start
- Link-down
- Link-up

Enterprise-specific traps are not currently supported by DataSMART MAX.

#### Warm-start trap

The warm-start trap is generated every time you enter **ESNMP** (enable SNMP) from the command-line and the agent was previously disabled.

#### Cold-start trap

The cold-start trap is generated every time the DataSMART MAX is power-cycled. Cold-start traps are not generated until ten seconds after the unit is power-cycled to allow the hardware providing the low level IP network interface time to start up and stabilize before attempting to send a packet.

#### Link-down trap

A link-down trap is generated when *ifOperStatus* (MIB II) changes to *down*.

#### Link-up trap

A link-up trap is generated when *ifOperStatus* (MIB II) changes to *up*.

## MIB objects included in SNMP traps

SNMP allows any MIB objects to be included in a trap. DataSMART MAX includes information on the status of the unit and the T1 line to speed analysis. Each trap type includes different information.

### Warm-start trap

A warm-start trap includes the *ifDesc* and *ifIndex* of all the interfaces on the unit.

### Cold-start trap

A cold-start trap includes the *ifDesc* and *ifIndex* of all the interfaces on the unit.

### Link-down trap for a T1 interface

A link-down trap for a T1 interface includes the following:

- *ifDesc* — “T1 Terminal Interface” or “T1 Network Interface”
- *ifIndex* — this is the instance number for that interface
- *dsx1LineStatus* — a bitmap of the T1 line’s current state
- *dsx1CurrentESs* — the number of errored seconds for the current interval
- *dsx1CurrentUASs* — the number of unavailable seconds for the current interval

### Link-down trap for a data port interface

A link-down trap for a data port interface includes the following:

- *ifDesc* — “Data Port *n* Interface” where *n* is the number of the data port
- *ifIndex* — this is the instance number for that interface

### Link-up trap for a T1 interface

A link-up trap for a T1 interface includes the following:

- *ifDesc* — “T1 Terminal Interface” or “T1 Network Interface”
- *ifIndex* — this is the instance number for that interface
- *dsx1LineStatus* — a bitmap of the T1 line’s current state
- *dsx1CurrentESs* — the number of errored seconds for the current interval
- *dsx1CurrentUASs* — the number of unavailable seconds for the current interval

### Link-up trap for a data port interface

A link-up trap for a data port interface includes the following:

- *ifDesc* — “Data Port *n* Interface” where *n* is the number of the data port
- *ifIndex* — this is the instance number for that interface

## Traps and Alarm Conditions

The following table correlates unit and alarm conditions to traps.

Alarm Condition	Trap
NI LOS	Link down port 1
NI OOF	Link down port 1
NI AIS	Link down port 1
NI YEL	Link down port 1
NI EER	Link down port 1
TI LOS	Link down port 2
TI OOF	Link down port 2
TI AIS	Link down port 2
TI YEL	Link down port 2
TI EER	Link down port 2
DPn LOS	Link down port <i>n</i>
Agent-enabled	Warm-start trap
Power-up	Cold-start trap

Where port *n* can be data port 3 – 6 (data ports 1 – 4).

---

## MIBs supported by DataSMART MAX

The DataSMART MAX internal SNMP agent supports sets, gets, and traps. SNMP sets and gets allow you to monitor and configure the unit, and traps alert you to error conditions with the unit, or the T1 line.

The DataSMART MAX supports three MIBs: an enterprise MIB and two industry-standard MIBs. All three MIBs are available on-line (see [page 9](#) for FTP site access).

The enterprise MIB allows you to configure the DataSMART MAX and view performance and status information with the same level of functionality as on the control port menus.

The two industry-standard MIBs supported by DataSMART MAX are: MIB II as defined in RFC 1213; and the DS1/E1 MIB, as defined in RFC 1406. MIB II contains information about the TCP/IP network interface on DataSMART MAX. The DS1/E1 MIB is the industry standard MIB for managing DS1 lines.

For a complete listing of the DataSMART MAX MIBs, refer to your *DataSMART MIB Reference* manual.

# 8

## *Quick reference*

---

This chapter contains:

- A listing of all menus and commands available through the command-line interface
- A flowchart of all menus and commands available through the front-panel interface
- A summary of commands accessible through an **ARC** login
- A description of how the DataSMART MAX generates T1 alarms, based on signal conditions at the network and terminal interfaces
- A complete listing of the DataSMART MAX specifications

---

## Command-line menus and commands

The command-line interface provides eighteen “help” menus. These menus group the various commands by function and describe the use and syntax of each command.

To display a menu, simply enter the one- or two-letter acronym for the menu title.

### Main menu (MM)

```
DataSMART MAX T1 4 Port A/D Ver. 1.31 Copyright (c) 1995-96 Kentrox
      ADDRESS: 00:00:000      NAME: PORTLAND,OR

MM          - Main Menu
SS          - System Status and Remote Menu
R           - Reports Menu

LM          - Local Maintenance Menu
RM          - Remote Maintenance Menu

AC          - Alarm Configuration Menu
CC          - Control Port Configuration Menu
DC          - Data Port Configuration Menu
FC          - Fractional T1 Configuration Menu
MC          - Management Configuration Menu
NC          - NI Configuration Menu
PC          - Password Entry and Configuration Menu
SC          - System Configuration Menu
TC          - T1 Configuration Menu

^D          - Logout
^D<xx>:<yy>:<zz>^E - Address Another Unit
```

### System Status and Remote menu (SS)

```
                                SYSTEM STATUS AND REMOTE MENU

ARC/DRC     - Access to/Disconnect from Remote Unit Control
S           - System Status Screen Command
DPLED<n>    - Select LED display of Data Port, n=1..4

SSV         - View System Setup
```



## Reports menu (R)

```
REPORTS MENU

UNSR / UNLR - User NI Short/Long Performance Report
UTSR / UTLR - User TI Short/Long Performance Report
CNSR / CNLR - Carrier NI Short/Long Performance Report
FESR / FELR - Far End PRM Short/Long Performance Report

NSR:[z]      - User NI Statistical Performance Report
TSR:[z]      - User TI Statistical Performance Report
              z = Display Report then Zero Counts (Optional)
AHR          - Alarm History Report

PL:<len|style> - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
              <style> = P (Page Break), M (More), or V (View)
```

## Local Maintenance menu (LM)

```
LOCAL MAINTENANCE MENU

SLL - Set Line Loop Back
SPL - Set Payload Loop Back
SLO - Set Local Loop Back
STI - Set TI Loop Back
SDP<n> - Set Data Port Loop Back at Data Port, n=1..4
SDT<n> - Set Data Terminal Loop Back at Data Port, n=1..4
RLB - Reset Loop Backs

DST - Do Self Test
```

## Remote Maintenance menu (RM)

```
REMOTE MAINTENANCE MENU

SRL          - Set Remote Line Loop Back
SRP          - Set Remote Payload Loop Back
SRDP<n>      - Set Remote Data Port Loop Back, n = 1 .. 4
RST1        - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1 ,0
S5C<n>      - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>      - Send 2047 Test Code in Data Port <n> Bit Stream
RTC         - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1 ,0
BT5<n>      - Activate BERT using 511 at Data Port n = 1 .. 4
BT2<n>      - Activate BERT using 2047 at Data Port n = 1 .. 4
```

## Alarm Configuration menu (AC)

```
ALARM CONFIGURATION MENU

EAM / DAM    - Enable/Disable Alarm Messages
EUM / ESM    - User/SNMP Alarm Message Format

EYL / DYL    - Enable/Disable YELLOW Activating an Alarm
DACT:<n>     - Alarm Deactivation time in seconds, n = 1..15
EST:<n>      - Errored Second Threshold, n = 0 .. 900
UST:<n>      - Unavailable Second Threshold, n = 0 .. 900
ST15/ ST60   - Set Threshold Timing to 15 or 60 Minutes

ACV          - View Alarm Configuration
```

## Control Port Configuration menu (CC)

```
CONTROL PORT CONFIGURATION MENU

EE / DE - Enable/Disable Character Echo
DCE/DTE - Select the Control Port
CCV      - View Control Port Configuration
```

## Data Port Configuration menu (DC)

```
DATA PORT CONFIGURATION MENU

EDI<n> / DDI<n> - Enable/Disable Data Inversion at Data Port, n=1..4
INTF<n>:<intf> - Interface at Data Port, n=1..4
                intf = V (V.35), E (EIA-530)
SCLK<n>:<clk> - Source Clock at Data Port, n=1..4
                clk = I (Internal), E (External)
TCLK<n>:<cmd> - Transmit Clock Inversion at Data Port, n=1..4
                cmd = E (Enable), D (Disable)
RCLK<n>:<cmd> - Receive Clock Inversion at Data Port, n=1..4
                cmd = E (Enable), D (Disable)
IDL<n>:<char> - Idle Character at Data Port, n=1..4
                char = 7E (0x7E), 7F (0x7F), FF (0xFF)
DPLOS<n>:<los> - LOS Input Signal at Data Port, n=1..4
                los = R (RTS), D (DTR), B (Both), N (No Processing)
DCV          - View Data Port Configuration
```

## Fractional T1 Configuration menu (FC)

```

FRACTIONAL T1 CONFIGURATION MENU

<table>DP<port>:<rate>[,<nicn>]
    table A/B      - DP=Assign NI Channel Map for Data Port
    port 1 .. 4    - Tables A or B Containing Channel Assignment
    rate 56/64     - Data Port Number
    nicn 1 .. 24   - Channel Rate in 1000 bps
    nicn 1,3,5,... - NI Channel numbers assigned to Data Port or
    1-24          - Can be alternating DS0 channel numbers or
                  - a contiguous range.

<table>NI<nicn>:<tict>,<nicn>:<tict>, ...
    table A/B      - NI=Assign NI Channels to TI or IDLE
    nicn 1 .. 24   - Tables A or B Containing Channel Assignment
    tict V,D,I    - NI Channel numbers
    tict V,D,I    - Voice/Data on TI Channel or I for Idle

CPAB / CPBA      - Copy A to B or B to A
LXA / LXB        - Load and Execute Table A or B
TAV / TBV        - View Table A or B
TXV              - View Executing Channel Assignment

```

## Management Configuration menu (MC)

```

MANAGEMENT CONFIGURATION MENU

ESNMP/DSNMP      - Enable/Disable SNMP Agent
TCS:<str>         - Set SNMP Trap Comm String, str=1 to 15 characters
RCS:<str>         - Set SNMP Read Comm String, str=1 to 15 characters
WCS:<str>         - Set SNMP Write Comm String, str=1 to 15 characters
TPW:<str>         - Set Telnet Password, str=0 to 15 characters
                  - 0 characters disables Telnet
SSA:<c>           - Set Packet Screening via Source Address
                  - c = (IP Addr), N (None)
NETIF:<c>         - Set IP Network Interface
                  - c = N (None), S (SLIP), E (Ethernet), B (Both)
IPR:<ipa>         - Set DSU Default Route IP Address
IPA:<c><ipa>       - Set DSU IP Addresses
IPM:<c><mask>      - Set DSU IP Mask
                  - c = S (SLIP), E (Ethernet)
ADD:<list>,<ipa>  - Add Address to Screening or Trap Dest Lists
DEL:<list>,<ipa>  - Delete Address to Screening or Trap Dest Lists
                  - <list> = I (IP Addr), T (Trap)
                  - <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
MCV              - View Management Configuration

```

## Network Interface Configuration menu (NC)

```
NI CONFIGURATION MENU

NSF/NESF/NERC - NI SF/ESF/Ericsson Framing Format
NAMI / NB8    - NI AMI/B8ZS Line Coding
EPRM / DPRM   - Enable/Disable T1.403 PRM Generation out NI
EYEL / DYEL   - Enable/Disable YELLOW Activation out NI
ADR54:<Trgt>   - 54016 Address = C(CSU), D(DSU), or B(Both)
E54 / D54     - Enable/Disable 54016 Mode

Line Build Out
NL0           - 0.0 dB
NL1           - 7.5 dB
NL2           - 15.0 dB

NCV           - View NI Configuration
```

## Password Entry and Configuration menu (PC)

```
PASSWORD ENTRY AND CONFIGURATION MENU

EPS:<password> - Enter Password
               password = 6 to 12 characters

APS:<access>:<password> - Add Password
                       access  = SA - Super User
                               CA - Configuration
                               MA - Maintenance
                       password = 6 to 12 characters

DPS:<password> - Delete Password
               password = 6 to 12 characters, or * for all

PUV           - View User Access Privilege
PCV           - View Password Configuration
```

## System Configuration menu (SC)

SYSTEM CONFIGURATION MENU	
SD:<mm>,<dd>,<yy>	- Set Date (Warning: This also clears reports)
ST:<hh>,<mm>	- Set Time (Warning: This also clears reports)
SN:<id>	- Set Name
SA:<xx>,<y/y>,<zzz>	- Set the Unit's Address to slot:shelf:group
EFP / DFP	- Enable/Disable Front Panel Operation
EDC / DDC	- Enable/Disable DataSMART compatibility
CLK:<src>	- Clock Source, src = L (Loop), T (TI Receive), I (Internal), E (External), <n> (Data Port at n=1..4)
ALGOUT:<n>	- Autologout, n = 0 .. 60 minutes
ZALL	- Zero All Counters used in User Reports
MCSWDL	- Download program from memory card
WYV	- View "What's Your Version" Information
RSD	- Reset System to Default Values
SCV	- View System Configuration

## Terminal Interface Configuration menu (TC)

TI CONFIGURATION MENU	
TSF/TESF/TERC	- TI SF/ESF/Ericsson Framing Format
TAMI / TB8	- TI AMI/B8ZS Line Coding
TIDL:<c>	- Idle Code, c = 00-FF Hex
TI Equalization	
TE0	- 0 - 133 ft
TE1	- 133 - 266 ft
TE2	- 266 - 399 ft
TE3	- 399 - 533 ft
TE4	- 533 - 655 ft
TCV	- View TI Configuration

# Front-panel menus and commands

In the flowcharts below, movement through the front-panel interface is denoted as follows:

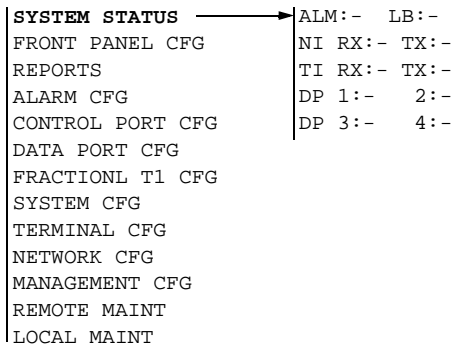
- A vertical line to the left of a column represents a menu listing that you cycle through by pushing the Next or Previous button.
- A vertical line to the right of a column means that each item in the list has the same entry path into the next menu or command (listed to the left).
- An arrow represents a path you enter by pushing the Select button, and exit by pushing the Escape button.
- Bold face type represents a specific path through the interface, starting at the top of the menu hierarchy.

You cycle through command fields by pushing the Next or Previous button. You select field values by pushing the Select button.

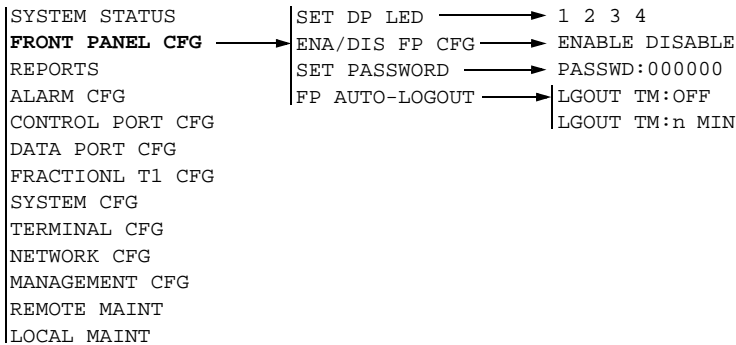
You can always escape to the top of the menu hierarchy by pushing the Escape button repeatedly.

If the front-panel is disabled, it defaults to a display of %EFS (error-free seconds).

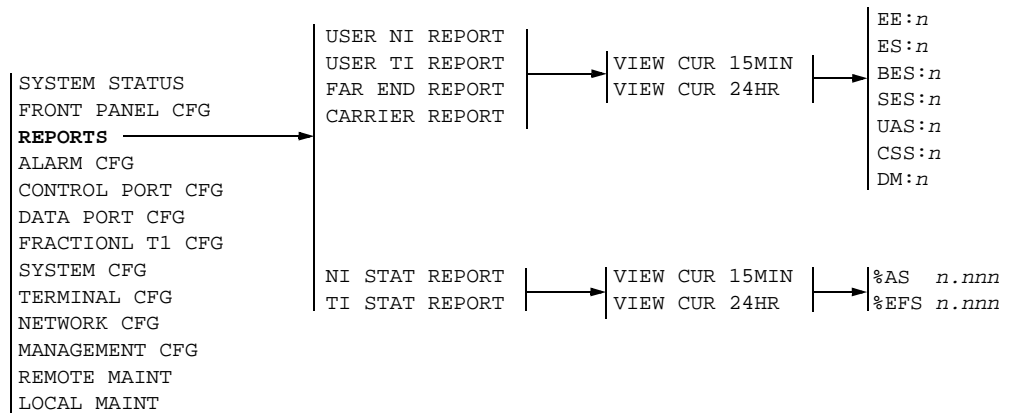
## System status



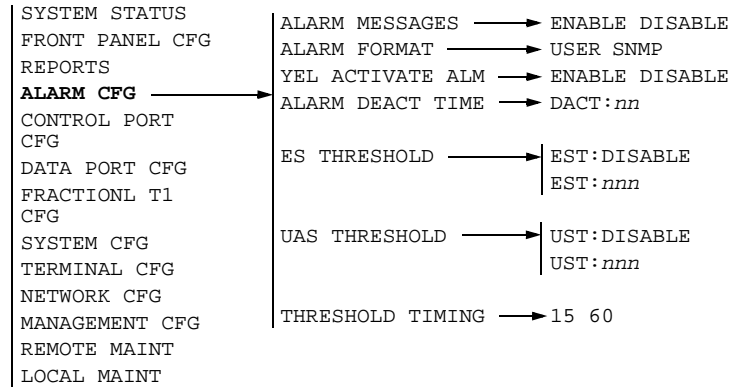
## Front-panel configuration



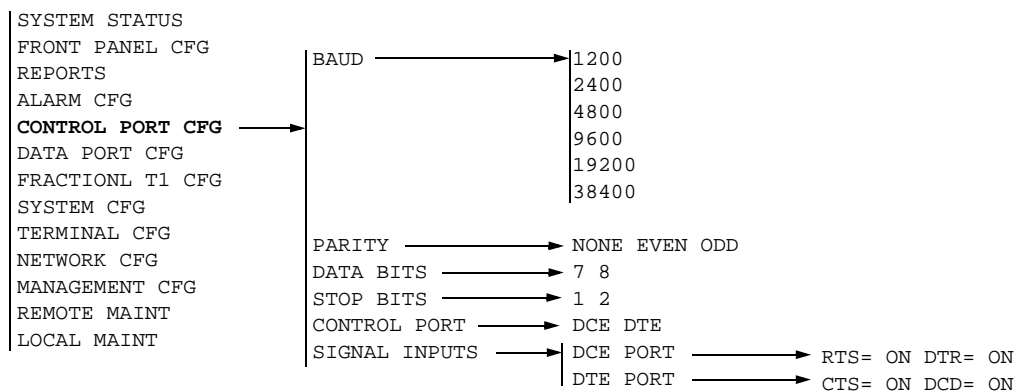
## Reports



## Alarm configuration

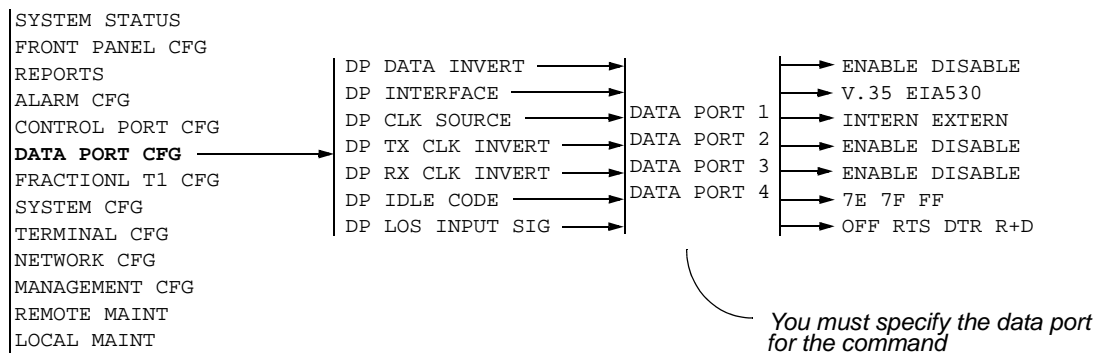


## Control port configuration

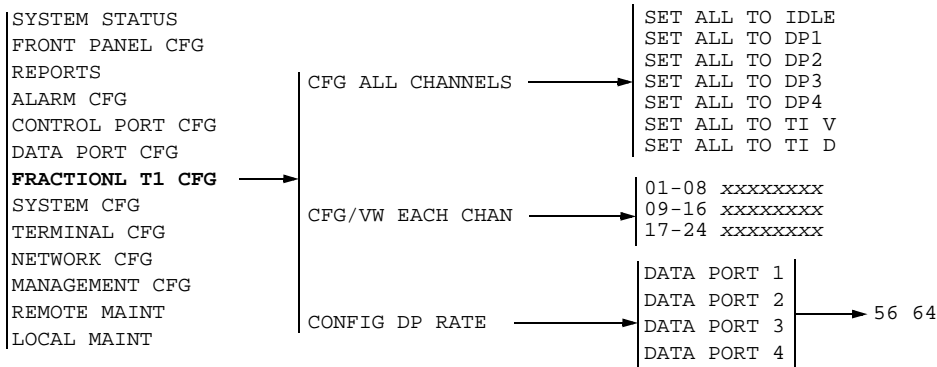




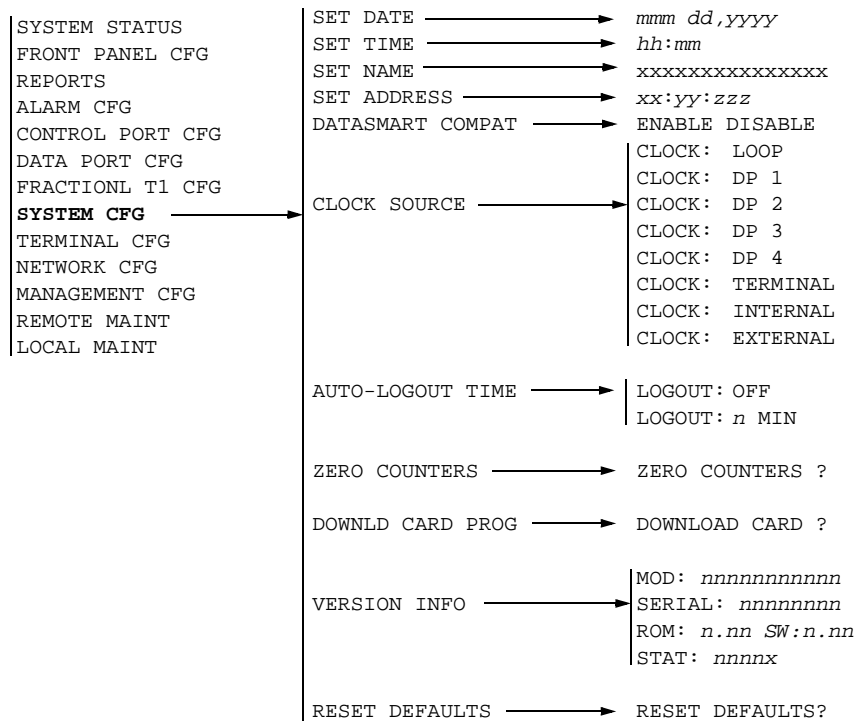
Data port configuration



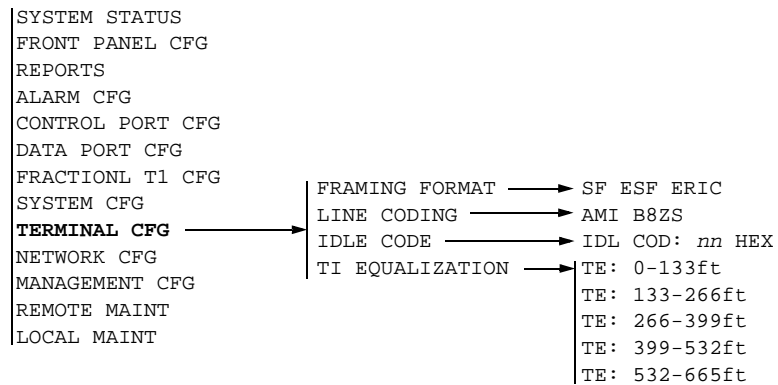
Fractional T1 configuration



## System configuration



## Terminal configuration



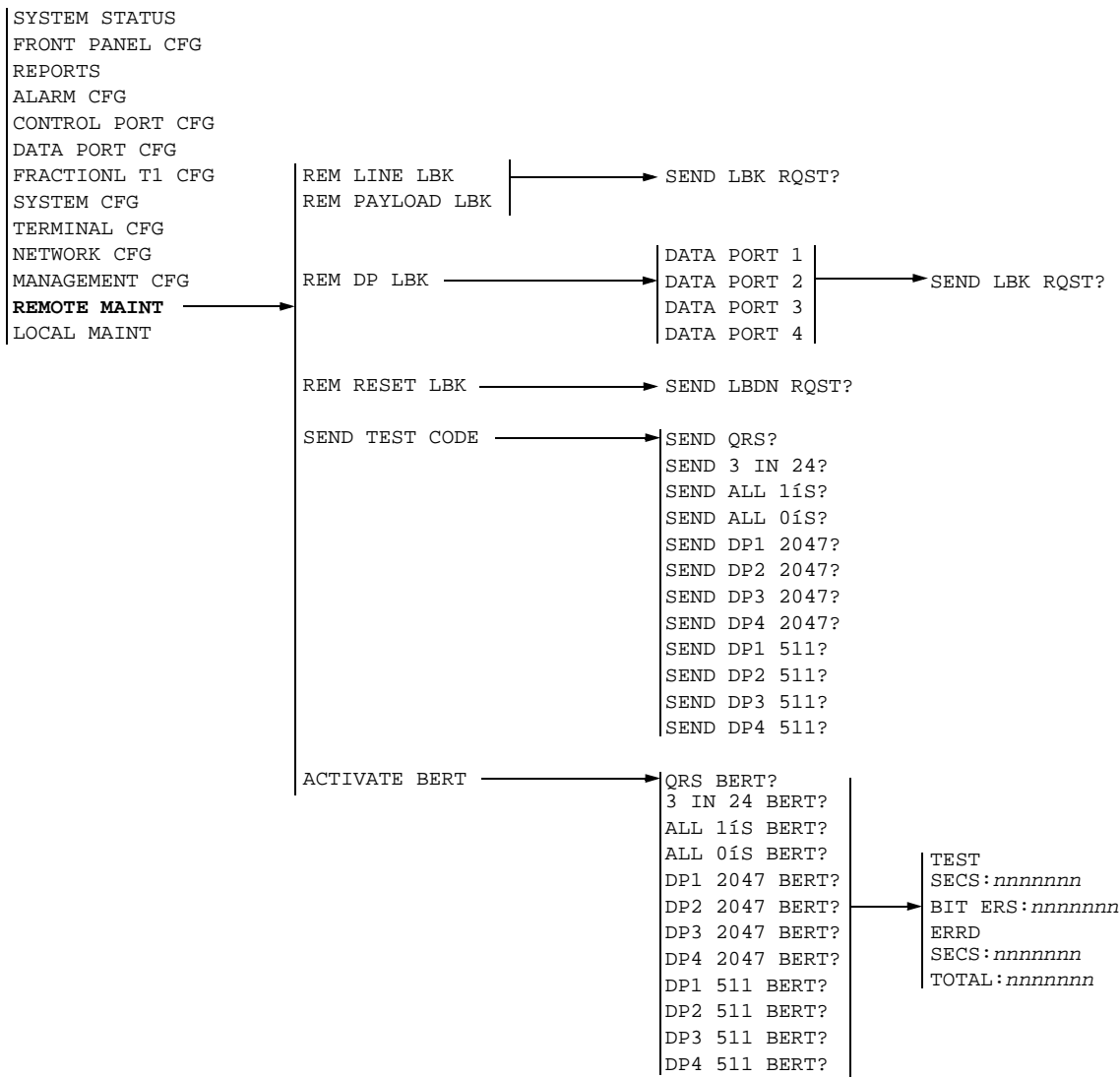
## Network configuration

SYSTEM STATUS	
FRONT PANEL CFG	
REPORTS	
ALARM CFG	
CONTROL PORT CFG	
DATA PORT CFG	
FRACTIONL T1 CFG	
SYSTEM CFG	
TERMINAL CFG	
<b>NETWORK CFG</b>	FRAMING FORMAT —→ SF ESF ERIC
MANAGEMENT CFG	LINE CODING —→ AMI B8ZS
REMOTE MAINT	54016 ADDRESS —→ CSU DSU BOTH
LOCAL MAINT	54016 MODE —→ ENABLE DISABLE
	PRM GENERATION —→ ENABLE DISABLE
	YEL GENERATION —→ ENABLE DISABLE
	LBO: 0.0
	LINE BUILD OUT —→ LBO: 7.5
	LBO: 15.0

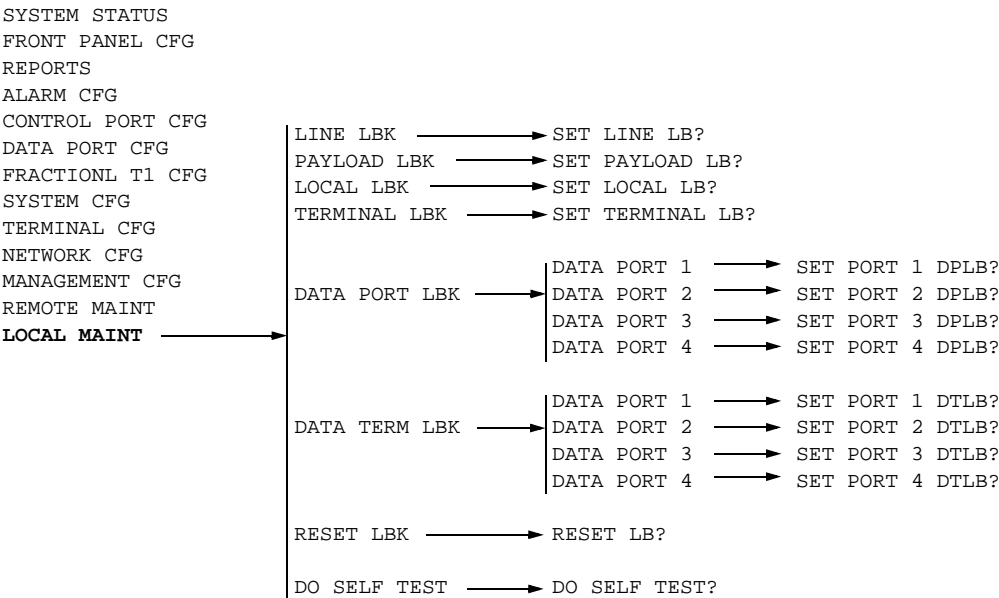
## Management configuration

SYSTEM STATUS	
FRONT PANEL CFG	
REPORTS	
ALARM CFG	
CONTROL PORT CFG	
DATA PORT CFG	
FRACTIONL T1 CFG	
SYSTEM CFG	
TERMINAL CFG	
NETWORK CFG	
<b>MANAGEMENT CFG</b>	SNMP AGENT —→ ENABLE DISABLE
REMOTE MAINT	TRAP COM STRING —→ xxxxxxxxxxxxxxxx
LOCAL MAINT	READ COM STRING —→ xxxxxxxxxxxxxxxx
	WRITE COM STRING —→ xxxxxxxxxxxxxxxx
	TELNET PASSWORD —→ xxxxxxxxxxxxxxxx
	SRC ADDR SCREEN —→ IP_ADDR NONE
	IP NETWORK INTF —→ NONE SLP ETH BOTH
	DSU DEFLT ROUTE —→ nnn.nnn.nnn.nnn
	SLIP IP ADDRESS —→ nnn.nnn.nnn.nnn
	SLIP IP MASK —→ nnn.nnn.nnn.nnn
	ETHER IP ADDRESS —→ nnn.nnn.nnn.nnn
	ETHER IP MASK —→ nnn.nnn.nnn.nnn
	ADD TRAP ADDR —→ nnn.nnn.nnn.nnn
	ADD SCREEN ADDR —→ nnn.nnn.nnn.nnn
	DEL/VW TRAP ADDR —→ nnn.nnn.nnn.nnn
	DEL/VW SCRIN ADDR —→ nnn.nnn.nnn.nnn

Remote maintenance



Local maintenance



---

## Commands available via ARC

You can log into a remote DataSMART MAX unit or a remote DataSMART unit by using the **ARC** command. This command establishes the remote login via the FDL (facility data link) line in the T1 signal. The T1 framing format must be ESF (extended super frame). The **DRC** command disconnects the remote login.

The **ARC** command's actions are affected by the **EDC/DDC** commands. The default power-up value is DataSMART MAX.

### **EDC (enable DataSMART compatibility) command**

Use the **EDC** command prior to executing **ARC** to specify that you are connecting to a DataSMART unit. Executing **EDC** has the following effects:

- Remote data loopbacks: all SRDP data port commands and the next RST1 command following SRDP generate the  $\overline{127}$  code in a format compatible with DataSMART. The code is transmitted continuously for 10 seconds or until the loop action is verified.
- T1.403 remote payload loopbacks: if the DataSMART MAX is the remote unit, then the DataSMART MAX does not expect loopback retention codes to be transmitted from the remote unit.

### **DDC (disable DataSMART compatibility) command**

Use the **DDC** command to disable DataSMART compatibility. Executing **DDC** has the following effects:

- Remote data loopbacks: all SRDP commands and the next RST1 command following SRDP generate the code in a format compatible with Annex B of T1.403-1994. The code is transmitted for approximately 2.5 seconds, followed by a transmission of all ones lasting approximately 2.5 seconds. Since the remote unit is required to perform the loop activity within 2 seconds of receiving the all-ones code, the DataSMART MAX sends a momentary loop code again after the 2.5 seconds of all ones to confirm the loop actions. If ten seconds elapses before the loop action is verified, the loop is considered unverified. Setting and resetting remote data port loopbacks may not be reliable if this setting is incorrect.
- T1.403 remote payload loopbacks: the DataSMART MAX expects retention codes as defined in T1.403-1994. If they are not received (as from a DataSMART unit) the unit actuates the loopback and immediately resets it.

# DataSMART MAX compatibility

You can access most DataSMART MAX commands via an ARC remote login. The only commands you cannot access are those that could potentially break the FDL link, or those that set up the network interface and the terminal interface in an add/drop unit. The commands that you cannot access through **ARC** are:

DataSMART MAX menu	Commands <i>not</i> accessible via ARC
System Status menu	EDC, DDC
Local Maintenance menu	DST, SDP, SDT, SLL, SLO, SPL, STI
Remote Maintenance menu	BTC, SRP, SRL, SRDP, S/C, RTC, RST1
NI Configuration menu	NAMI, NB8, NERC, NESF, NLx, NSF
System Configuration menu	MCSWDL
TI Configuration menu	TAMI, TB8, TERC, TE1, TE2, TE3, TE4, TESF, TSF

# DataSMART compatibility

You can execute only a subset of the DataSMART commands via an ARC remote login. The subset consists of the commands found on the DataSMART Control Port Configuration menu and on its Status and Remote menu.

DataSMART menu	Commands accessible via ARC	Command functions
System Status and Remote menu	S	System Status Screen command
Fractional T1 Configuration menu	CPA/CPB	Copy A to B or B to A
	LXA/LXB	Load and execute table A or table B
	TAV/TBV	View table A or table B
	TXV	View executing channel assignment
	<table>DP	Assign channels to data port
	<table<NI>	Assign channels to terminal or idle

- The FC command works only when a DataSMART MAX is the local unit. The FC command returns a DataSMART DC menu from a DataSMART and a DataSMART MAX FC menu from a DataSMART MAX.
- The DC command returns an FC menu from a DataSMART MAX and a DC menu from a DataSMART.

---

## T1 alarms and signal processing

This section describes how the DataSMART MAX transitions into and out of an alarm state. It also describes in detail the alarms that can occur at the network and terminal T1 interfaces and the signal conditions that cause them.



### NOTE

*For a complete listing of all alarms generated by the DataSMART MAX and appropriate troubleshooting procedures, refer to Chapter 6, “[Troubleshooting](#)”.*

### What happens when alarms occur

When the DataSmart MAX transitions to an alarm state, it performs various actions:

- It illuminates appropriate LEDs on the front panel.
- It updates the System Status display with status information about the alarms and signal conditions at the network interface, terminal interface, and data ports.
- It outputs an SNMP trap or an alarm message to the control device (if traps or messages are enabled) and logs the alarm message in the Alarm History report.
- It transmits yellow alarms and idle code out the interfaces and data ports as appropriate.
- It switches the clock source to internal master timing, if the condition obstructs the clocking source.

### How alarms are generated

The DataSMART MAX generates alarms based on error events that occur in an input signal. Error events are also referred to as signal conditions. For instance, a loss of signal event (LOS) is also referred to as an LOS signal condition. A signal condition is a current, instantaneous status of the received signal at the interface. The signal condition may persist, may be intermittent, or may disappear immediately.

If a signal condition persists or is intermittent but frequent, the DataSMART MAX transitions into an alarm state, a process called “alarm integration.” The algorithm that controls alarm integration is designed to prevent alarms from being raised every time a signal condition occurs briefly, and to prevent the alarm from being deactivated every time the signal condition temporarily flickers off.

#### The alarm integration algorithm

The alarm integration algorithm uses two values: the alarm integration time and the decay rate. (On the DataSMART MAX the alarm integration time is set to 2.5 seconds and the decay rate is 1/5.)

The algorithm maintains a count for each signal condition. Whenever a signal condition exists, time accrues to the count for that signal condition. For instance, if the OOF signal condition exists for 1 second, 1 second is accrued to the OOF count. Time spent out of the signal condition is multiplied by 1/5 (the decay rate) and subtracted from the count, which has a minimum value of 0. When the count exceeds 2.5 (the alarm integration time), the transition to an alarm state occurs.

The alarm integration algorithm is defined in detail in AT&T 62411.



## Transitioning out of the alarm state

When a signal condition that has produced an alarm goes away, the alarm persists until the condition has been absent for a period of time referred to as the alarm deactivation time. The alarm deactivation time is user-configurable and by default is 15 seconds. (See [“Setting the alarm deactivation time” on page 67](#) for more information.)

## Alarm reporting

The DataSMART MAX produces an alarm message each time a line transitions to a new alarm state. The “CLR” message is not sent until all alarms on a particular interface clear. All alarm messages are output to the device connected to the control port and are logged in the Alarm History report. To see the Alarm History report, type **AHR** at the command line.

You can examine the current status and track the changing conditions on an interface using the System Status report (type **S** at the command line). This report shows the current alarm state of the DataSMART MAX as well as the signal condition of the input and output signal at all interfaces. The status report is updated once a second upon any changes to the alarm state or signal conditions. You can also track system status from the LCD display on the front panel of the DataSMART MAX. See [“Examining system status” on page 129](#) for more information.

A received T1 signal is classified as being in one and only one alarm state at a time. Alarm states have a priority. If the signal satisfies more than one of the requirements for an alarm state, the higher priority alarm applies. Because of this, and because of the delay of deactivation of an alarm, the System Status report could contain an entry in which an interface is in an alarm state that does not match the signal condition.

For example, suppose the alarm deactivation time period is set to 15 seconds, and suppose the signal condition for the NI received signal is AIS. After the alarm integration requirements are met, the line is declared to be in the AIS alarm state. Now suppose that the signal condition changes from AIS to OOF. At this point the DataSMART MAX will add a new entry to the status report to show the change in the signal condition. However, in that same entry, the alarm condition will be shown as AIS because the alarm deactivation time period has not passed.

Now assume the OOF condition persists for 2.5 seconds, and thus has satisfied the conditions for alarm integration. Because the OOF has a lower priority, and because of the 15-second deactivation period for alarms, the alarm state will still be AIS. However, once the 15 seconds have passed, the alarm state will transition from AIS to OOF, and the DataSMART MAX will add a new entry to the status report.

## Signal conditions

The table below lists the signal conditions for the DataSMART MAX in priority order, highest priority first. A received T1 signal can be in one and only one of the signal conditions at a time.

Condition	Definition
LOS	Loss of Signal. No pulses are being received. The LOS signal condition starts upon receipt of 192 consecutive spaces or zeros. The LOS signal condition clears when a the signal contains 32 consecutive bits with at least 4 ones and no more than 15 consecutive zeros.

Condition	Definition
AIS	Alarm Indication Signal. A signal with a 99.9% ones density for a minimum of 3 milliseconds and no framing detected is being received. The AIS condition is detected in the presence of a $1 \times 10^{-3}$ bit error rate. An AIS condition is declared when both out-of-frame and all 1s conditions are present at the interface. The AIS condition clears when either the OOF, all 1s, or both conditions clear.
OOF	Out of Frame. The received signal does not contain a T1 framing pattern. The OOF signal condition is declared when two out of four frame bits are in error (SF and Ericsson framing) or when two out of six frame bits are in error (ESF framing). The OOF signal condition clears when a reframe occurs.
EER	Excessive Error Rate. A framed T1 signal with a event error rate exceeding the user-supplied threshold is being received. This condition clears when the next time interval's error count is less than the threshold.
YELLOW	The received signal contains the yellow alarm pattern in bit two of each DS0 (SF framing) or a yellow alarm code word in the ESF Data Link (ESF framing). The condition clears when the yellow alarm pattern is no longer detected in the received signal.
Good Signal	A framed T1 signal with none of the above listed signal conditions.

## Alarms

For each of the signal conditions described in the previous table there is an alarm state. The table below lists the alarms for the DataSMART MAX in priority order, highest priority first. Note that, as shown in the table, not all alarms use the alarm integration algorithm described on page [200](#).

Alarm	Definition
LOS	The LOS alarm starts upon a total of 2.5 seconds of alarm integration time spent in the LOS signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent LOS signal condition). The LOS alarm clears after a continuous time period of $n$ seconds with no LOS signal condition, where $n$ is the alarm deactivation time period set by the user via the DACT command.
AIS	The AIS alarm starts upon a total of 2.5 seconds of alarm integration time spent in the AIS signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent AIS signal condition). The AIS alarm clears after a continuous time period of $n$ seconds with no AIS signal condition, where $n$ is the alarm deactivation time period set by the user via the DACT command.
OOF	The OOF alarm starts upon a total of 2.5 seconds of alarm integration time spent in the OOF signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent OOF signal condition). The OOF alarm clears after a continuous time period of $n$ seconds with no OOF signal condition, where $n$ is the alarm deactivation time period set by the user via the DACT command.

Alarm	Definition
Yellow Alarm	The yellow signal alarm is declared after receiving the yellow signal for 1 second. Once declared, the alarm stays active for a minimum of one second. It is cleared upon detection of an input signal without the yellow alarm pattern present.
EER	The EER alarm starts immediately upon entering the EER signal condition. The EER alarm clears after a continuous time period of $n$ seconds with no EER signal condition, where $n$ is the alarm deactivation time period set by the user via the DACT command.
Clear	None of the above listed alarms is active.

# Specifications

**Table 7— Environmental Specifications**

	Parameter	Specification
<b>Temperature</b>	Storage	-20°C to 66°C (5% to 65% RH)
	Operating	0°C to 50°C (5% to 90% RH, non-condensing)
<b>Powering</b>	AC input range	85 to 265 VAC, 47 to 63 Hz (when optioned with AC power)
	DC input range	20 to 56 VDC tolerance included (when optioned with DC power)
	Power interruptions	Loss of power does not damage the unit. Loss of power for less than five years does not change the configuration settings which may have been set by the user. Loss of power for less than ten hours (nominal) does not affect any of the performance data collected by the unit or time of day.

**Table 8— Physical Specifications**

	Parameter	Specification
	Size with feet	2.120 inches by 17 inches by 11.5 inches
	Size without feet	1.720 inches by 17 inches by 11.5 inches
	Weight	Approximately 6 pounds

**Table 9— Electrical interface specifications - Network Interface**

	Parameter	Specification
<b>Common</b>	Line rate	Internal or external clock; 1.544 Mb/s $\pm$ 50 bps When timing is derived from input signal: 1.544 Mb/s $\pm$ 200 bps. Output line rate follows input line rate.
	Line Code	AMI or B8ZS (selectable).
	Line Impedance	100 ohms $\pm$ 10 ohms at 772 kHz 100 ohms $\pm$ 20% over the frequency band 100 kHz to 1Mhz
	Lightning Protection	Lightning surges defined per FCC Part 68 shall not damage the unit
	Framing Format	SF or ESF per ANSI T1.403-1989, and TR-54016-1989; Ericsson Framing (defined as valid F <sub>T</sub> bits only)
<b>Input Only</b>	Input Level	DSX-1 to -27.5 dB.
	Input Jitter Tolerance	Per TR 62411-1990 (p. 4.7.1)

**Table 9— Electrical interface specifications - Network Interface (continued)**

	Parameter	Specification
<b>Output Only</b>	Output Level	Per ANSI T1.403-1989 3.0 Volt peak $\pm$ 10% into 100 ohms at output connector
	Output Signal	Tolerant to impedance mismatches.
	Line Build Out	0, 7.5, 15.0 selectable
	Output Jitter	TR 62411-1990 (p 4.7.2)
	Jitter Transfer	DSU: TR 62411-1990 (p 4.7.3) ADD/DROP: PUB 43802
	Pulse Density	(When enabled) shall be > 12.5%
<b>Network Interface Connector</b>	15-pin male D connector	
	RxD Data (T1)	Pin 3
	RxD Data (R1)	Pin 11
	TxD Data (T)	Pin 1
	TxD Data (R)	Pin 9
	Frame Ground	Pins 2 and 4
	Not Used	Pins 5, 6, 7, 8, 10, 12, 13, 14, 15
<b>Note</b>	Simplex Current	Simplex current is looped to the network in normal configuration. If it becomes necessary to change this configuration, contact Kentrox Technical support.

**Table 10— Electrical interface specifications - Terminal Interface**

	Parameter	Specification
<b>Common</b>	Line rate	Internal: 1.544 Mb/s $\pm$ 32 ppm When timing is derived from input signal: 1.544 Mb/s $\pm$ 200 bps. Output line rate follows input line rate.
	Line Code	AMI or B8ZS (selectable).
	Line Impedance	100 ohms $\pm$ 10 ohms at 772 kHz 100 ohms $\pm$ 20% over the frequency band 100 kHz to 1Mhz
	Framing Format	SF or ESF per ANSI T1.403-1989 (p. 6), and TR-54016-1989 (p 4.1); Ericsson Framing (defined as valid F <sub>T</sub> bits only) Idle ESF Data Link is set to 1s.
<b>Input Only</b>	Input Level	DSX-1 to -10.0 dB
	Input Jitter Tolerance	per TR 62411-1990 (p. 4.7.1)
	Input Jitter Transfer	per TR 62411-1990 (p. 4.7.2)
<b>Output Only</b>	Output Level	DSX-1 at connector (no equalization enabled).
	Equalization	Up to 655 feet selectable, 5 steps.
<b>Terminal Interface Connector</b>	15-pin female D connector	
	RxD Data (T1)	Pin 3
	RxD Data (R)	Pin 11
	TxD Data (T)	Pin 1
	TxD Data (R1)	Pin 9
	Frame Ground	Pins 2 and 4
	Not Used	Pins 5, 6, 7, 8, 10, 12, 13, 14, 15

**Table 11— External Clock Specification**

	Parameter	Specification
<b>Connector</b>	RS-422 A	Pin 1
	RS-422 B	Pin 2
<b>Signal</b>	Frequency	1544 KHz signal
	Electrical	RS-422
	Duty cycle	50%/50% $\pm$ 10

**Table 12— Serial Control Port Specification**

	Parameter	Specification
	Baud Rate	1200, 2400, 4800, 9600, 19200
	Electrical Interface	EIA-574
<b>Connector</b>	DCE	DB9S
	DTE	DB9P

**Table 13—Control port pin assignments**

CCITT	Pin	Signal name	DTE	DCE
125	9	Ring Indicator (RI)	INPUT	OUTPUT
109	1	Rec Sig Det (DCD)	INPUT	OUTPUT
108.2	4	DTE Ready (DTR)	OUTPUT	INPUT
102	5	Signal GND		
104	2	Received Data	INPUT	OUTPUT
103	3	Transmit Data	OUTPUT	INPUT
106	8	Clear To Send (CTS)	INPUT	OUTPUT
105	7	Request To Send (RTS)	OUTPUT	INPUT
107	6	Data Set Ready (DSR)	INPUT	OUTPUT

**Table 14— Data Port Interface Specification**

Parameter	Specification
Bit Rates	56 kHz to 1536 kHz
Connector	25-pin D connector - adaptable to V-35 or EIA-449 (subset) with cable adapters
Electrical Interfaces	EIA-530: Per ANSI/EIA-530A-1992 V.35: Compatible.
Interface Type	DCE

**Table 15—DB25D connector pin assignments for EIA-530**

<b>Pin</b>	<b>Designator CCITT/EIA</b>	<b>Circuit name</b>	<b>Source</b>
1	—	Shield	—
2	(a) 103/BA	BA (A), Transmitted Data	DTE
3	(a) 104/BB	BB (A), Received Data A	DCE
4	(a) 105/CA	CA (A), Request To Send A (RTS)	DTE
5	(a) 106/CB	CB (A), Clear To Send A (CTS)	DCE
6	107/CC	CC (A), DCE Ready (DSR)	DCE
7	102/AB	AB, Signal Ground	DTE
8	(a) 109/CF	CF (A), Received Line Signal Detector	DCE
9	(b) 115/DD	DD (B), Receiver Signal Element Timing	DCE
10	(b) 109/CF	CF (B), Received Line Signal Detector	DCE
11	(b) 113/DA	DA (B), Transmit Signal Element Timing	DTE
12	(b) 114/DB	DB (B), Transmit Signal Element Timing	DCE
13	106/CB	CB (B), Clear To Send	DCE
14	(b) 103/BA	BA (B), Transmitted Data	DTE
15	(a) 114/DB	DB (A), Transmit Signal Element Timing	DCE
16	(b) 104/BB	BB (B), Received Data	DCE
17	(a) 115/DD	DD (A), Receiver Signal Element Timing	DCE
18		Not supported	
19	(b) 105/CA	CA (B), Request To Send	DTE
20	108.2/CD	CD (A), DTE Ready	DTE
21		Not supported	
22	(b) 107/CC	CC (B), DCE Ready	DCE
23	108.2/CD	CD (B), DTE Ready	DTE
24	113/DA	DA (A), Transmit Signal Element Timing	DTE
25	142/TM	TM, Test Mode	DCE



**Table 16—DB25D connector pin assignments for V.35**

<b>Pin</b>	<b>CCITT</b>	<b>Circuit name</b>	<b>Source</b>
1		Protective GND	
2	(a) 103	Tx Data A	DTE
3	(a) 104	Rx Data A	DCE
4	105	RTS	DTE
5	106	CTS	DCE
6	107	DSR	DCE
7	102	Signal GND	
8	109	Rec Line Sig Det (DCD)	DCE
9	(b) 115	Rx Timing B	DCE
10		No used	
11	(b) 113	External clock B	DTE
12	(b) 114	Tx Timing B	DCE
13		Not used	
14	(b) 103	Tx Data B	DTE
15	(a) 114	Tx Signal Timing A	DCE
16	(b) 104	Rx Data B	DCE
17	(a) 115	Rx Signal Timing A	DCE
18		Not supported	
19		Not used	
20	108.2	DTR	DTE
21		Not supported	
22		Not supported	
23		Not used	
24	(a) 113	External Clk A	DTE
25	142	Test Mode	DCE

**Table 17—V.35, DB25P connector to V.35, 34-pin connector adapter cable**

<b>DB25P Pins</b>	<b>34 Pin</b>	<b>Circuit name</b>
1	A	Protective GND
2	P	Tx Data A
3	R	Rx Data A
4	C	RTS or RR
5	D	CTS
6	E	DSR
7	B	Signal GND
8	F	Rec Line Sig Det (DCD)
9	X	Rx Signal Timing B
10		Not connected
11	W	External Clk B
12	AA	Tx Signal Timing B
13		Not connected
14	S	Tx Data B
15	Y	Tx Signal Timing A
16	T	Rx Data B
17	V	Rx Signal Timing A
18	L	Future
19		Not connected
20	H	DTR
21	N	Future
22		Not connected
23		Not connected
24	U	External Clk A
25	NN	Future

**Table 18— DB25S connector to RS449, 37-pin connector adapter cable**

<b>EIA-530 DB25S Pins</b>	<b>RS449 DB37 Pins</b>	<b>Circuit name</b>
1	—	Protective ground
2	4	Tx data A
3	6	Rx data A
4	7	RTS
5	9	CTS
6	11	DSR
7	19	Signal GND
8	13	Rec line sig det (DCD)
9	26	Rx signal timing B
10	31	Rec line sig det (DCD)
11	35	External clk B (DTE source)
12	23	Tx signal timing B
13	27	CTS
14	22	Tx data B
15	5	Tx signal timing A
16	24	Rx data B
17	8	Rx signal timing A
18	Not Supported	
19	25	RTS
20	12	DTR
21	Not Supported	
22	29	DSR
23	30	DTR
24	17 (DTE source)	External clk A
25	Not Supported	

**Table 19—Compatibility**

Standard
AT&T TR54016 Issue 2, (TR62411/1990)
AT&T TR54019 Appendix A (Fractional T1)
EIA T1.403/1994
TIA-547

**Table 20— Supported loopbacks**

Loopback	Definition
LLB Line loopback	A minimum penetration loopback at the NI interface.
PLB, Payload loopback	An interior loopback, looping the payload back to the NI.
DPLB(n), Data Port loopback	Looping the bit stream assigned to the designated data port back towards the NI.
DTLB(n) Data Terminal loopback	Looping the bit stream back to the data terminal equipment connected to the data port.
LOC Local loopback	An interior loopback, looping only the payload back to the Terminal Interface or data ports.
TILB Terminal Interface loopback	A minimum penetration loopback at the TI interface.

# Glossary

---

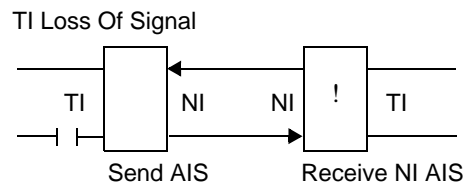
**2047** A test code pattern used for fractional T1 line testing.

**3 in 24** A test code pattern used for testing a full T1 line.

**511** A test code pattern used for fractional T1 line testing.

**add/drop** A device in which channels from the T1 line at the network interface can be assigned to either a data port or a T1 line at the terminal interface.

**AIS** Alarm Indication Signal. A signal condition and alarm indicating that the signal has been lost somewhere upstream. When a device experiences a loss of signal, it transmits an AIS signal to the next device downstream.



**alarm** An unsolicited message from a device that typically indicates a problem with a line.

**all 0s** A test code pattern used for testing a full T1 line.

**all 1s** A test code pattern used for testing a full T1 line.

**auto-logout** A feature that automatically logs out a user if there has been inactivity for a specified length of time.

**BERT** Bit Error Rate Test. A utility that is used to isolate faulty lines. To troubleshoot a line, the first step is to send a test pattern (often utilizing a loopback to return the code to the device that initiated the test). BERT analyzes the signal to see if the line has caused errors in the pattern. By progressively testing segments of the circuit, the tester can discover which portion of the line is causing the problem.

**BPV** Bipolar Violation. An error event on a line in which the normal pattern of alternating high and low signals is disrupted. A bipolar violation is when two high signals occur without an intervening low signal, or vice versa.

**carrier** A company, such as any of the “baby Bell” companies, that provide network communications services, either within a local area or between local areas.

**CCS** Common channel signaling.

<b>channel</b>	A single communication path created, in the case of a T1 line, by multiplexing. A T1 line carries 24 channels, each with a bandwidth of 64 Kbps.
<b>cold-start trap</b>	An SNMP trap that is sent when the unit has been power-cycled. <i>See also</i> trap.
<b>command-line interface</b>	One method for accessing the management functions of the DataSMART MAX, characterized by typing commands at a video display terminal. <i>See also</i> front-panel interface.
<b>control port</b>	A port, either DTE or DCE, on the DataSMART MAX to which you can connect a terminal, modem, or SLIP device, and that provides access to the DataSMART MAX management functions. Control ports are also used to daisy-chain DataSMART MAX units.
<b>controlled slip</b>	A situation in which one frame's worth of data is either lost or replicated. A controlled slip typically occurs when a DataSMART MAX is not using the same clock as the unit that generated the received signal.
<b>CPE</b>	Customer Premise Equipment. Equipment that is on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. <i>See also</i> point of demarcation.
<b>CRC</b>	Cycle Redundancy Check.
<b>CTS</b>	Clear To Send. Hardware flow-control on a control port or data port. DataSMART MAX can be set to monitor the data port for assertion of CTS. In this mode, if CTS is not asserted, a data port loss of signal alarm is generated.
<b>daisy-chain</b>	A string of DataSMART MAX units that have been interconnected so that they can all be managed from one terminal.
<b>data port</b>	A port on a DSU to which some or all of the channels of a DS1 line can be routed.
<b>datagram</b>	A packet of information used in a connectionless network service that is routed to its destination using an address included in the datagram's header.
<b>DCE</b>	Data Communications Equipment. A definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.
<b>DS1</b>	A standard that specifies an interface operating at 1.544 mbps (million bits per second) and 24 discrete data channels that runs on a T1 line. In common usage, DS1 is synonymous with T1.
<b>DSU/CSU</b>	Data Service Unit/Channel Service Unit. A DSU is a device that makes the link between a T1 line and a line that is carrying packetized data streams such as those produced by a router. A CSU is a device that makes the link between a T1 line and a line that is carrying raw data streams such as those produced by a PBX. A DSU/CSU combines the two functionalities.

**DTE** Data Terminal Equipment. A definition in the RS-232C standard that describes the functions of the signals and the physical characteristics of an interface for a terminal device such as a terminal.

**DTR** Data Terminal Ready. Hardware flow-control on a control port or data port. DataSMART MAX can be set to monitor the data port for assertion of DTR. In this mode, if DTR is not asserted, a data port loss of signal alarm is generated.

**ECF** External Clock Input Failure. An alarm generated by DataSMART MAX that is configured for external clocking and has lost the clocking signal.

**EER** Excessive Error Rate. An alarm which indicates that a threshold for the number of errored seconds or unavailable seconds has been exceeded.

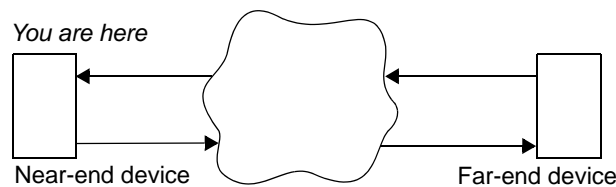
**embedded SNMP agent** An SNMP agent can come in two forms: embedded or proxy. An embedded SNMP agent is one that is integrated into the physical hardware and software of the unit. DataSMART MAX has an internal, integrated SNMP agent. Advantages to this approach are time-accuracy of data and fast response time. See also proxy SNMP agent.

**EQF** Internal Equipment Failure. Something has happened to cause the internal hardware of the DataSMART MAX to fail. The unit needs to be serviced.

**ES** Errored Second. A measurement of the quality of the signal on a T1 line defined as any second that is not an unavailable second and that contains one or more CRC6 errors.

**ESF** Extended Super Frame.

**far-end** In a relationship between two devices in a circuit, the far-end device is the one that is remote.



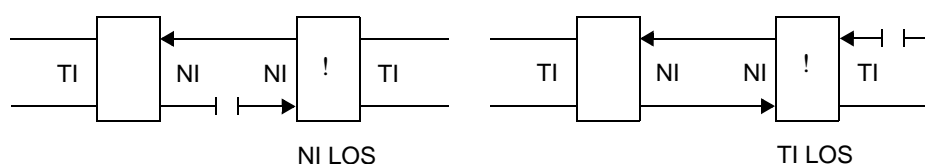
**FDL** Facility Data Link. A link embedded in the ESF framing bits that is used for such things as accessing performance data on remote units, remote log in, and carrier access to the DataSMART MAX.

**fractional T1** A service in which the carrier provides only a subset of the full 24 channels of a T1 line.

**Frame Relay** A packet-oriented communication protocol.

**frame slip** See controlled slip.

<b>front-panel interface</b>	A way to access the management functions of the DataSMART MAX using an LCD display and four push buttons on the front-panel of the DataSMART MAX.
<b>ICMP</b>	Internet Control Message Protocol. ICMP is a protocol in the TCP/IP suite of protocols that is used to determine if a host is alive and responding. An ICMP query is referred to as a Ping. The response is either an “I can hear you” message, or simply no response. DataSMART MAX will respond to Ping requests, but does not generate them.
<b>IP</b>	Internet Protocol. A suite of protocols for packetizing data for shipment across LANs and WANs. Protocols exist above the IP protocol for transmitting and receiving IP packets. DataSMART MAX uses the IP protocol to provide SNMP and Telnet access.
<b>IP address</b>	A unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in “dot” notation; for instance, 192.228.32.14. <i>See also</i> IP netmask.
<b>IP netmask</b>	A pattern of 32 bits that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for sub-dividing IP networks. IP netmasks are written in “dot” notation; for instance, 255.255.255.0. <i>See also</i> IP address.
<b>link-down trap</b>	An SNMP trap that signifies that the T1 line has transitioned from a normal state to an error state, or that a data port has been disconnected.
<b>link-up trap</b>	An SNMP trap that signifies that the T1 line, or a data port has transitioned from an error condition to a normal state.
<b>LOFC</b>	Loss of Frame Count. An LOFC is the accumulation of the number of times a Loss of Frame is declared. On detection of an LOS or OOF, a rise-slope type integration process starts that declares a Loss of Frame after 2.5 ( $\pm 0.5$ ) seconds of continuous LOS or OOF. If the LOS or OOF is intermittent, the integration process decays at a slope of 1/5 the rise slope during the period when the signal is normal. Thus, if the ratio of an LOS or OOF to a normal signal is greater than 1/5, a Loss of Frame is declared. If during a one-second interval, but no more than 15 contiguous one-second intervals, no LOS or OOF conditions occur, the Loss of Frame condition is cleared.
<b>loopback</b>	A troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.
<b>LOS</b>	Loss Of Signal. A signal condition and alarm in which the received signal at the network interface or the terminal interface is lost.

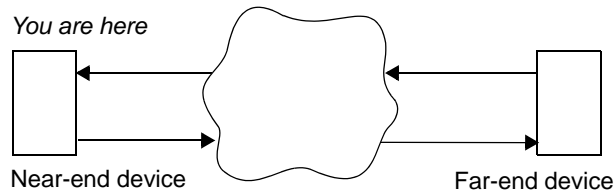




**MIB** Management Information Base. The information that SNMP can access, structured as a hierarchy. In common usage of the word, MIB is in reference to a sub-branch of the entire MIB. DataSMART MAX uses the MIB II and the DS1 MIB.

**modem** Modulator/demodulator. A device for converting a digital signal to analog (and vice versa) so that it can be transmitted over phone lines.

**near-end** In a relationship between two devices in a circuit, the near-end device is the one that is local.



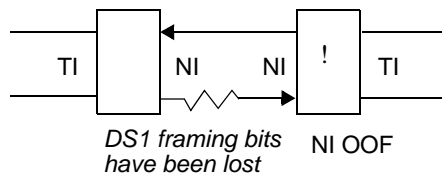
**NI** Network interface. The interface between the DataSMART MAX and the T1 line supplied by the carrier.

**NMS** Network Management System. A tool for configuring network devices and monitoring network performance, typically an SNMP-based tool.

**OID** Object Identifier. The address of a MIB variable.

**ones density** A characteristic of a T1 line that refers to the rate at which 1s occur on the line. Because devices such as the DataSMART MAX cannot track a bit pattern using 0s, it loses synchronization if the 1s density is not high enough.

**OOF** Out of frame. An signal condition and alarm in which some or all of DS1 framing bits are lost.



**PBX** Private Branch Exchange. A private telephone switch-bank. A company will generally have a few numbers that dial into a PBX and from there the switchboard operator can direct the call to a particular extension. Phone calls within the company do not need to go outside of the PBX to be switched. Larger PBXs often have T1 interfaces to connect to one or more CSUs.

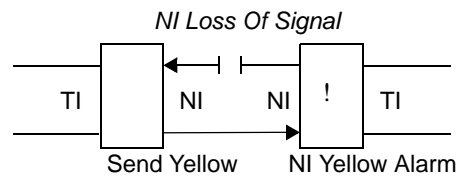
**PCMCIA** Personal Computer Memory Card International Association. DataSMART MAX has a PCMCIA card slot into which an Ethernet card can be plugged, providing connectivity to an IP network via Ethernet.

<b>ping</b>	A protocol that is part of the TCP/IP suite, used to test the connectivity of the network. Ping sends a signal to a host or gateway, then listens for an echo response.
<b>point of demarcation</b>	The dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.
<b>PRM</b>	Performance Report Message. Messages that are received once per second from a far-end device that report information about the condition of the far-end device.
<b>proxy SNMP agent</b>	SNMP agents come in two forms: embedded and proxy. A proxy agent is physically outside of the device being managed. The proxy is a translator between the device's native command language and SNMP. Advantages of proxy agents are management of legacy equipment which cannot support embedded SNMP agents, and management of large numbers of devices where network connections may be limited. See also embedded SNMP agent.
<b>QRS</b>	Quasi-Random Signal. A test code pattern used for testing a full T1 line.
<b>real-time clock</b>	A clock that maintains the time of day in distinction to a clock that is used to time the electrical pulses on a circuit.
<b>RJ45</b>	A type of cable connector used for RS-232 lines and 10BaseT Ethernet lines.
<b>router</b>	A device that connects various links in a network matrix, directing packets along the most economical or efficient routes to the packet's destination; a packet switch.
<b>RxD</b>	Received Data. The control ports and data ports on DataSMART MAX have an RxD line. This line is defined from the DTE perspective, so RxD for a DCE port is actually TxD. Each data port has a pair of RxD and TxD LEDs on the front panel. See also TxD.
<b>SF</b>	Super Frame.
<b>signal condition</b>	Characteristics of the electronic pulses on a line, categorized into groups of various error types. When errored signal conditions persist they cause a DataSMART MAX to raise an alarm.
<b>SLIP</b>	Serial Line Interface Protocol. A protocol that allows the Internet Protocol (IP) to run on low-speed serial lines.
<b>SMDS</b>	Switched Multi-Megabit Digital Service. A public, high-speed, connectionless, packet-switched data transfer service that provides LAN-like performance and features over an entire metropolitan area.
<b>SNMP</b>	Simple Network Management Protocol. The accepted industry-standard network manage-

ment protocol that uses a system of agents and managers. Each agent is responsible for interacting with a certain MIB. The manager can ask the agent for data, or it can ask the agent to set the value of some data.

<b>super-user</b>	A login ID that allows unlimited access to the full range of a device's functionality, especially including the ability to reconfigure the device and set passwords.
<b>T1</b>	A specification for a transmission line. The specification details the input and output characteristics and the bandwidth. T1 lines run at 1.544 Mbps and provide for 24 data channels. In common usage, the term "T1" is used interchangeable with "DS1."
<b>TCP</b>	Transport Control Protocol. TCP is one of the two transport protocols in the TCP/IP protocol suite. TCP is a complex, connection-based protocol that guarantees reliable delivery of packets. Telnet uses TCP.
<b>TCP/IP</b>	A suite of protocols that includes IP, UDP, TCP, SNMP, TELNET, ICMP, and PING. TCP/IP is the networking protocol of choice of the Internet and many private networks as well. Kentrox SNMP and Telnet products operate in TCP/IP networks.
<b>Telnet</b>	Telnet is a TCP/IP protocol that defines a client/server mechanism for emulating directly-connected terminal connections. DataSMART MAX implements a Telnet Server, allowing other devices to establish connections with it. DataSMART MAX does not implement a Telnet Client (which would allow DataSMART MAX to connect to other devices).
<b>terminal server</b>	In the simplest terms, a terminal server is an IP network port and a collection of serial ports. Most terminal servers allow the serial ports to be configured for SLIP. If DataSMART MAX is using SLIP for its IP network connection, a terminal server could be used to make the connection from serial to ethernet.
<b>TI</b>	Terminal Interface. The interface between the DataSMART MAX and the T1 line on the customer premise.
<b>trap</b>	A trap is an unsolicited alert generated by SNMP. There are five standard trap types: link up, link down, warm start, cold start, and enterprise-specific.
<b>TxD</b>	Transmit Data. The control ports and data ports on DataSMART MAX have a TxD line. This line is defined from the DTE perspective, so TxD for a DCE port is actually RxD. Each data port has a pair of RxD and TxD LEDs on the front panel. <i>See also</i> RxD.
<b>UAS</b>	Unavailable Seconds. A measurement of the signal quality of a T1 line. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.
<b>UDP</b>	User Datagram Protocol. One of the two transport protocols in the TCP/IP protocol suite. UDP is a send and forget protocol, which means there is no guarantee that the datagram will reach its destination.
<b>VDT</b>	Video Display Terminal.

- warm-start trap** One of the five SNMP trap types. For Kentrox equipment, warm start traps indicate that SNMP alarm messages or agents have been enabled.
- Xon/Xoff** This is software flow control for the control ports. When DataSMART MAX has too much data coming in, it will transmit an Xoff (stop transmitting) character. If the device on the other end understands flow control, it will stop transmitting until it receives an Xon (resume transmitting) character. If DataSMART MAX receives an Xoff, it stops transmitting data until it receives an Xon. Xon/Xoff flow control is not available when SLIP is enabled.
- yellow alarm** An alarm that occurs on a device when the signal from the device is not received at the far-end.



# Index

---

## Symbols

- %AS percentage of available seconds, 115
- %BES percentage of bursty errored seconds, 115
- %CSS percentage of controlled slip seconds, 115
- %DM percentage of degraded minutes, 115
- %EFS percentage of error-free seconds, 115
- %ES percentage of errored seconds, 115
- %SES percentage of severely errored seconds, 115

## Numerics

- 54016 address command, 76
- 54016 mode disable command, 77
- 54016 mode enable command, 77

## A

- AC alarm configuration menu
  - command, 59, 186
- access privileges, 32
- ACTIVATE BERT command, 154
- ACV view alarm configuration
  - command, 60
- ADD add IP address to list command, 166
- ADD add IP address to SNMP trap list
  - command, 176
- add password command, 31
- ADD SCREEN ADDR command, 166
- ADD TRAP ADDR command, 176
- add/drop example, 15
- ADDR54 54016 address command, 76
- address of device command, 43
- addresses, IP, 160
- AHR alarm history report command, 201
- alarm actions during, 200
- alarm activation on yellow disable
  - command, 63
- alarm activation on yellow enable
  - command, 63

- ALARM CFG command, 60, 192
- alarm configuring, 59
- alarm configuring commands
  - ACV view alarm configuration, 60
  - DACT alarm deactivation time, 67
  - DAM disable alarm messages, 61
  - EAM enable alarm messages, 61
  - ESM SNMP alarm formatting, 62
  - EUM ASCII alarm formatting, 62
  - ST15/ST60 threshold evaluation, 66
- ALARM DEACT TIME command, 67
- alarm deactivation time command, 67
- alarm history report, 118, 201
- alarm integration, 200
- alarm list
  - DPn LOS loss of DTR/RTS, 128
  - ECF external clock failure, 128
  - EQF equipment failure, 128
  - NI AIS incoming AIS, 128
  - NI EER excessive error rate, 128
  - NI LOS loss of T1 signal, 128
  - NI OOF T1 signal out of frame, 128
  - NI YEL incoming yellow, 128
  - TI AIS incoming AIS, 128
  - TI LOS loss of T1 signal, 128
  - TI OOF T1 signal out of frame, 128
  - TI YEL incoming yellow, 128
- alarm message disable command, 61
- alarm message enable command, 61
- ALARM MESSAGES command, 61
- alarm messages monitoring, 128
- alarm reporting, 201
- alarm states, 202
- alarm status codes, 130
- alarms generated list of, 128
- ALGOUT auto-logout command, 49
- applications, 14–15
- APS add password command, 31
- ARC remote login command, 26, 146, 183
- ASCII alarm formatting, 62
- assigning channels, 96, 98, 99, 102
- auto-logout command, 33, 36, 49
- AUTO-LOGOUT TIME command, 49
- auto-logout, control port, 48
- auto-logout, front panel, 49

## B

- BAUD command, 56
- BERT test codes commands, 152
- BERT test codes using, 150, 151, 152
- BES bursty errored seconds, 110, 113
- bipolar violations at a port, 138
- BTx BERT test codes commands, 152

## C

- carrier NI long perform report
  - command, 106
- carrier NI short perform report
  - command, 106
- CARRIER REPORT command, 120
- CC control port configuration menu
  - command, 187
- CCV view control port configuration
  - command, 54
- channel assignments (current) display
  - command, 100
- channels assigning, 96, 98, 99, 102
- CLK set source clock command, 47
- CLOCK SOURCE command, 48
- clock, system, 44
- CNLR carrier NI long perform report
  - command, 106
- CNSR carrier NI short perform report
  - command, 106
- command line interface
  - how to use it, 20–21
  - list of menus, 184–190
  - password protection, 30–32
- compatibility with DataSMART, 44, 199
- configuring alarms, 59
- configuring control port, 53
- configuring daisy-chained units for
  - Telnet access via Ethernet, 157
- configuring daisy-chained units for
  - Telnet access via SLIP, 156
- configuring data ports, 85
- configuring for SNMP, 173
- configuring for SNMP traps, 179
- configuring interfaces from table, 102
- configuring IP addresses, 160
- configuring IP netmasks, 160

- configuring network interface, 70
- configuring network management for Telnet, 156
- configuring SNMP trap hosts, 176
- configuring stand-alone units for management via Telnet, 156
- configuring terminal interface, 79
- control port alarm messages at, 128
- CONTROL PORT CFG command, 54, 192
- CONTROL PORT command, 58
- control port configuring, 53, 54
- control port physical connection, 56
- control port pinouts, 207
- control port specify command, 57
- controlled slips, 135
- conventions used in the manual, 11
- copy table A to B command, 102
- copy table B to A command, 102
- counters, zeroing, 50
- CPAB copy table A to B command, 102
- CPBA copy table B to A command, 102
- CRC-6 errors alarm, 138
- CSS controlled slip seconds, 110, 113

## D

- D54 54016 mode disable command, 77
- DACT alarm deactivation time command, 67
- daisy-chain, 16, 26, 39, 43, 156, 157, 171
- daisy-chain controller (SLIP or Ethernet), 18
- daisy-chain, control ports, 57
- daisy-chain, logging in, 44
- daisy-chain, logging out, 44
- daisy-chain, viewing the current configuration, 54
- DAM alarm message disable command, 61
- DATA BITS command, 56
- data inversion disable command, 87
- data inversion enable command, 87
- DATA PORT CFG command, 85, 193
- data port clocking, 89
- data port commands
  - data port idle character, 93
  - data port interface command, 88
  - data port LED select command, 124
  - data port loopback set command,

- 146
- data port LOS state command, 94
- data port source clock command, 90
- data port configuring, 85
- data port idle character, 93
- data port LED, 124
- data port loopback, 143
- data port LOS, 136
- data port LOS processing, 94
- data port receive clock inversion, 92
- data port status codes, 133
- data port transmit clock inversion, 91
- data terminal loopback set on data port *n*, 146
- date and time setting, 40
- date command, 40
- DC data port configuration menu command, 187
- DCE, DTE specify control port command, 57
- DCV view data port configuration command, 86
- DDC disable DataSMART compatibility command, 198
- DDI disable data inversion command, 87
- DE disable echo character command, 57
- default router, 163
- default values reset command, 51
- DEL delete address from SNMP trap lists command, 177
- DEL delete IP address from list command, 168
- DEL/VW SCRNR ADDR command, 169
- DEL/VW TRAP ADDR, 177
- delete password command, 31
- DFP disable front panel command, 36
- diagnostics, 19
- DM degraded minutes, 111, 113
- DO SELF TEST command, 139
- DP CLK SOURCE command, 90
- DP DATA INVERT command, 87
- DP IDLE CODE command, 93
- DP INTERFACE command, 88
- DP LOS alarm at a data port, 136
- DP LOS INPUT SIG command, 95
- DP RX CLK INVERT command, 92
- DP TX CLK INVERT command, 91
- DPLED data port LED select command, 124

- DPLOS data port LOS state command, 94
- DPRM disable PRM and loopback command, 74
- DPS delete password command, 31
- DRC remote logout command, 26
- DSNMP disable SNMP agent command, 173
- DST do self-test command, 139
- DSU DEFLT ROUTE command, 163
- DSU example, 14
- DSU IP ADDRESS command, 160
- DSU IP MASK command, 160
- DSU with add/drop example, 15
- DTE, DCE specify control port command, 57
- DYEL disable yellow alarm output command, 75
- DYL alarm activation on yellow disable command, 63

## E

- E54 enable 54016 mode command, 77
- EAM alarm message enable command, 61
- ECF alarm, 135
- echo character disable command, 57
- echo character enable command, 57
- echo enable/disable, 57
- EDC DataSMART MAX/DataSMART ARC compatibility command, 213
- EDC enable DataSMART compatibility command, 198
- EDI enable data inversion command, 87
- EE enable echo character command, 57
- EE error events, 110, 112
- EFP enable front panel command, 36
- ENA/DIS FP CFG command, 35
- EPRM enable PRM and loopback command, 74, 112
- EPS enter password command, 32
- equalization TI specifying, 83
- errored seconds threshold command, 64
- ES errored seconds, 110, 112
- ES THRESHOLD command, 64
- ESM SNMP alarm formatting, 62
- ESNMP enable SNMP agent command, 173

EST errored seconds threshold  
command, 64  
Ethernet, 18, 157  
EUM ASCII alarm formatting, 62  
EYEL enable yellow alarm output  
command, 75  
EYL alarm activation on yellow  
enable command, 63

## F

facility data link (FDL), 18  
FAR END REPORT command, 120  
far-end report, 112  
FC fractional T1 configuration menu  
command, 188  
FELR performance report command,  
112  
FESR performance report command,  
112  
formatting reports, 107  
FP AUTO-LOGOUT command, 36  
Fractional T1, 14  
FRACTIONAL T1 CFG command,  
102, 193  
Frame Relay, 14  
FRAMING FORMAT command, 72,  
81  
framing format NI specifying, 71  
framing format TI specifying, 80  
FRONT PANEL CFG command, 35,  
124, 191  
front panel disable command, 36  
front panel enable command, 36  
front panel enable/disable command,  
35  
front panel interface  
how to use it, 21–25, 191  
introduction, 16  
list of commands, 191–197  
password protection, 33–36  
front panel security, 26  
front panel, auto-logout, 49

## I

ICMP Internet Control Message  
Protocol, 216  
IDL data port idle character command,  
93  
IDLE CODE command, 83  
idle code command, 82  
idle code TI specifying, 82

invert clock edge command, 91, 92  
IP address add to list command, 166  
IP address default router, 163  
IP address delete from list command,  
168  
IP address screening list, 166, 168  
IP address set command, 160  
IP address source screening, 166, 170  
IP addresses, 160  
IP netmask, 160, 161  
IP netmask set command, 162  
IP network interface, 171  
IP NETWORK INTF command, 172  
IP screening password set command,  
170  
IPA set IP address command, 160  
IPM set IP netmask command, 162  
IPR set default router command, 163

## J

jacks signal, 141

## L

LED data port, 124  
LED display abnormal, 125  
LED display normal, 125  
LEDs, 124–127  
LINE BUILD OUT command, 78  
line build out commands, 78  
line code TI specifying, 81  
LINE CODING command, 73, 82  
line coding NI specifying, 73  
line loopback set command, 146  
LM local maintenance menu  
command, 185  
load configuration from table A  
command, 102  
load configuration from table B  
command, 102  
local loopback set command, 146  
LOCAL MAINT command, 139, 147,  
196, 197  
logging in, 26, 44  
logging out, 27  
login remote command, 26, 139, 198  
logout remote command, 26, 198  
logout, auto command, 36  
logout, auto, command, 49  
logout, auto, control port, 48  
logout, auto, front panel, 49  
loopback commands

set data port loopback on data port *n*,  
146  
set data terminal loopback on data  
port *n*, 146  
set line loopback, 146  
set local loopback, 146  
set payload loopback, 146  
set remote line loopback, 148  
set remote loopback on data port *n*,  
148  
set remote payload loopback, 148  
set TI loopback, 146  
loopback data terminal, 144  
loopback dataport, 143  
loopback line, 142  
loopback local, 144  
loopback payload, 142  
loopback set reset remotely, 148  
loopback setting resetting in local  
device, 146  
loopback status codes, 131  
loopback terminal interface, 145  
loopbacks using, 142  
LOS processing data port, 94  
LXA load configuration from table A  
command, 102  
LXB load configuration from table B  
command, 102

## M

MANAGEMENT CFG command,  
158, 195  
MC management configuration menu  
command, 158, 188  
MCSWDL download control program  
command, 51  
MCV view management configuration  
command, 159  
MIB FTP site, 9  
MIB objects included in SNMP traps,  
180  
MIBs supported, 9, 182  
MM main menu command, 184  
monitoring alarm messages, 128  
multimedia access multiplexer, 13, 16

## N

name device command, 42  
NAMI network interface line coding  
command, 73  
NB8 network interface line coding

- command, 73
- NC network interface configuration
  - menu command, 189
- NCV view network configuration
  - command, 71
- NERC network interface framing
  - format command, 72
- NESF network interface framing
  - format command, 72, 112
- NETIF set network interface
  - command, 171
- netmasks, 160
- NETWORK CFG command, 70, 195
- network input status codes, 131
- network interface alarms
  - NI EER alarm, 136
  - NI LOS alarm, 134
  - NI OOF alarm, 135
  - NI YEL alarm, 137
- network interface configuring, 70
- network interface framing format
  - command, 72
- network interface line coding
  - command, 73
- network interface NI AIS alarm, 135
- network interface set command, 171
- network interface signal jacks, 141
- network output status codes, 132
- NI report carrier's, 119
- NI report display long command, 106
- NI report display short command, 106
- NI STAT REPORT command, 120
- NL0, NL1, NL2 line build out
  - commands, 78
- nonvolatile memory, 19
- NSF network interface framing format
  - command, 72
- NSR NI statistics report command,
  - 116, 117

## P

- PARITY command, 56
- password enter command, 32
- passwords, 30, 31, 32
- payload loopback set command, 146
- PC password entry and configuration
  - menu command, 189
- PCV view password configuration
  - command, 32
- performance monitoring, 18
- performance report commands, 112
- ping, 218

- pinouts
  - control port, 207
  - DB25S connector to RS449 adapter,
    - 211
  - external clock, 206
  - network interface, 205
  - terminal interface, 206
  - V.35 DB25D connector, 209
  - V.35 DS25S connector to V.35 34-
    - pin connector adapter cable,
      - 210
- PL format reports command, 107
- privileges, 32
- PRM and loopback disable command,
  - 74
- PRM and loopback enable command,
  - 74
- PRM GENERATION command, 74
- PUV view privilege command, 32

## R

- R reports menu command, 185
- RCLK invert clock edge command, 92
- RCS set SNMP strings command, 175
- READ COM STRING command, 175
- REM DP LBK command, 149
- REM LINE LBK command, 149
- REM RESET LBK command, 149
- remote loopback set on data port *n*,
  - 148
- remote loopback set on line, 148
- remote loopback set on payload, 148
- REMOTE MAINT command, 149,
  - 196
- report alarm history, 118
- report carrier's NI, 119
- report far-end interpreting, 112
- reports accessing, 106
- REPORTS command, 120, 192
- reports format command, 107
- reports formatting, 107
- reports interpreting, 108
- reports statistical interpreting, 114
- reports time intervals in, 108
- RESET DEFAULTS command, 52
- reset loopback command, 146
- reset to default values, 51
- RLB reset loopback command, 146
- RM remote maintenance menu
  - command, 186
- router, 163
- router set default command, 163

- RSD reset defaults command, 51, 107
- RTC reset test code generation
  - command, 152

## S

- S display system status command, 129
- SA set device address command, 43
- SC system configuration menu
  - command, 190
- SCLK data port source clock
  - command, 90
- SCV view current settings command,
  - 39
- SD set date command, 40, 107
- SDP set data port loopback command,
  - 146
- SDT data terminal loopback on data
  - port *n* command, 146
- self-test command, 139
- self-test diagnostics running, 139
- SEND TEST CODE command, 153
- SES severely errored seconds, 110,
  - 113
- SET ADDRESS command, 43
- SET DATE command, 41, 121
- SET DP LED command, 124
- SET NAME command, 42
- SET PASSWORD command, 34
- SET TIME command, 41, 121
- signal conditions, 201
- SIGNAL INPUTS command, 55
- signal jacks, 141
- SLIP, 18, 156
- slips controlled, 135
- SLL set line loopback command, 146
- SLO set local loopback command, 146
- SN name device command, 42
- SNMP
  - ADD IP address to SNMP trap list
    - command, 176
  - agent enable/disable, 173
  - configuring for SNMP, 173–177
  - configuring trap hosts, 176
  - DEL delete address from SNMP trap
    - lists command, 177
  - DSNMP agent disable command,
    - 173
  - ESNMP enable SNMP agent
    - command, 173
  - formatting alarms, 62
  - network management, 17
  - RCS set strings commands, 175



- setting community strings, 174
- SNMP AGENT command, 170, 174
- TCS set strings commands, 175
- trap address list, 177
- using traps, 179–181
- WCS set strings commands, 175
- SNMP agent enable command, 179
- source clock command, 47
- source clocking data port, 89
- SPL set payload loopback command, 146
- SRC ADDR SCREEN command, 170
- SRDP set remote loopback on data port *n* command, 148
- SRL set remote line loopback command, 148
- SRP set remote payload loopback command, 148
- SS system status and remote menu command, 184
- SSA set IP screening password command, 170
- ST set time command, 40, 107
- ST15 threshold evaluation window command, 66
- ST60 threshold evaluation window command, 66
- standard data interfaces, 16
- statistical reports, 114
- status codes alarm, 130
- status codes data ports, 133
- status codes loopback, 131
- status codes network input, 131
- status codes network output, 132
- status codes terminal input, 132
- status system codes list, 130
- STI set TI loopback command, 146
- STOP BITS command, 56
- SxC send test codes commands, 152
- SYSTEM CFG command, 38, 121, 194
- system clock, 44
- system parameters, specifying, 38
- system parameters, view current setting, 39
- system status codes list, 130
- SYSTEM STATUS command, 130, 191
- system status examining, 129

## T

- T1 diagnostics, 19

- T1 performance monitoring, 18
- table A display contents command, 100
- table B display contents command, 100
- TAMI terminal interface line coding command, 81
- TAV display table A command, 100
- TB8 terminal interface line coding command, 81
- TBV table B display contents, 100
- TC display TI configuration menu command, 79
- TC terminal interface configuration menu command, 190
- TCLK invert clock edge command, 91
- TCP/IP, 219
- TCS set SNMP strings command, 175
- TCV view TI configuration command, 80
- TE0,1,2,3,4 signal equalization command, 83
- Telnet, 156, 157
  - introduction, 26
  - password set command, 165
  - TELNET PASSWORD command, 165
- TERC terminal interface framing format command, 80
- TERMINAL CFG command, 79, 194
- terminal input status codes, 132
- terminal interface alarms
  - TI AIS alarm, 138
  - TI EER alarm, 137
  - TI LOS alarm, 134
  - TI OOF alarm, 136
  - TI YEL alarm, 137
- terminal interface configuring, 79
- terminal interface line coding commands, 81
- TESF terminal interface framing command, 80
- test code
  - 2047, 131, 132, 150, 152
  - 3 in 24, 131, 132, 150, 152
  - 511, 131, 132, 150, 152
  - all 0s, 131, 132, 150, 152
  - all 1s, 131, 132, 150, 152
  - QRS, 131, 132, 150, 152
- test code reset command, 152
- test codes
  - commands, 152

- threshold evaluation window
  - command, 66
- THRESHOLD TIMING command, 66
- TI configuration menu display
  - command, 79
- TI EQUALIZATION command, 84
- TI long, user perform report command, 106
- TI loopback set command, 146
- TI short, user perform report
  - command, 106
- TI STAT REPORT command, 120
- TIDL idle code command, 82
- time and date setting, 40
- time command, 40
- TPW set Telnet password command, 165
- TRAP COM STRING command, 175
- traps
  - alarm conditions and traps, 181
  - cold-start trap, 179, 180
  - enabling, 62
  - link-down trap, 179, 180
  - link-up trap, 179, 180
  - warm-start trap, 179, 180
- troubleshooting, 123
  - bipolar violations, 138
  - CRC errors alarm, 138
  - DP LOS alarm, 136
  - ECF alarm, 135
  - NI AIS alarm, 135
  - NI EER alarm, 136
  - NI LOS alarm, 134, 135, 136
  - NI OOF alarm, 135
  - NI YEL alarm, 137
  - TI AIS alarm, 138
  - TI EER alarm, 137
  - TI LOS alarm, 134
  - TI YEL alarm, 137
- TSF terminal interface framing format
  - command, 80
- TSR TI statistics report command, 116
- TXV current channel assignments
  - display command, 100

## U

- UAS THRESHOLD command, 65
- UAS unavailable seconds, 110, 113
- unavailable seconds threshold
  - command, 65
- UNLR display long NI report
  - command, 106

UNSR display short NI report  
command, 106

USER NI REPORT command, 120

UST unavailable seconds threshold  
command, 65

UTLR user TI long perform report  
command, 106

UTSR user TI short perform report  
command, 106

## V

VERSION INFO command, 51

version information command, 51

view alarm configuration command,  
60

view control port configuration  
command, 54

view current settings command, 39

view data port configuration  
command, 86

view network configuration command,  
71

view TI configuration command, 80

## W

WCS set SNMP strings command, 175

WRITE COM STRING command,  
175

WYV version information command,  
51

## Y

YEL ACTIVATE ALM command, 63

YEL GENERATION command, 75

yellow alarm output disable command,  
75

yellow alarm output enable command,  
75

## Z

ZALL zero counters command, 50,  
107

ZERO COUNTERS command, 50,  
121

zero counters command, 50